NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

CONCEPT FOR A SPECIAL OPERATIONS PLANNING AND ANALYSIS SYSTEM

by
Allan L.Bilyeu

June 1998

Thesis Advisor: Gordon H. Bradley
Second Reader: Charles H. Shaw, III

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1998	Master's Thesis

4. TITLE AND SUBTITLE CONCEPT FOR A SPECIAL OPERATIONS PLANNING AND ANALYSIS SYSTEM

5. FUNDING NUMBERS

6. AUTHOR(S) Bilyeu, Allan L.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Special Operations Command, J-7C
7701 Tampa Point Blvd
MacDill AFB, Tampa, FL 33621

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

ABSTRACT *(maximum 200 words)* This thesis designed and partially implemented a platform independent mission planning and analysis system for the United States Special Operations Command (USSOCOM). The ability to move to platform independent technologies is particularly meaningful for the special operations community that could never expect to move to a standardized computer planning system for their joint, multi-national, and inter-agency operations. This thesis also investigates the ability to integrate legacy systems in an open architecture on an object web. In addition, this thesis incorporates current operations research methods into this system to show their importance in planning and analysis. The system is developed in the Java programming language using the loosely coupled components architecture. The system involves an image component that contains a map with overlays. Discussion of an object web established using a common object request broker architecture (CORBA) integrating legacy systems ends this portion of the research. To show the relevance of this system, a scenario involving joint and coalition forces is developed. The scenario demonstrates the usefulness and need for platform independent planning and analysis systems. Finally, this thesis recommends an architecture that USSOCOM should investigate for its future mission planning, analysis, rehearsal, and execution (MPARE) system..

13. SUBJECT TERM
Java, Loosely Coupled Components, Map Based Planning, Special Operations,MPARE

15. NUMBER OF PAGES 82

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

CONCEPT FOR A SPECIAL OPERATIONS PLANNING AND ANALYSIS SYSTEM

Allan L. Bilyeu
Captain, United States Army
B.S., United States Military Academy, 1987

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
June 1998

Author: Allan L. Bilyeu

Approved by: Gordon H. Bradley, Thesis Advisor

Charles H. Shaw, III, Second Reader

Richard Rosenthal, Chariman
Department of Operations Research

ABSTRACT

This thesis designed and partially implemented a platform independent mission planning and analysis system for the United States Special Operations Command (USSOCOM). The ability to move to platform independent technologies is particularly important for the special operations community since it can not expect standardized computer planning and analysis systems for their joint, multi-national, and inter-agency operations. This thesis also investigates the ability to integrate legacy systems using an open architecture on an object web. In addition, this thesis incorporates operations research methods into this system to show their importance in planning and analysis. The system is developed in the Java programming language using loosely coupled components. The system involves an image component that contains a map with overlays. The use of common object request broker architecture (CORBA) for integrating legacy systems is discussed. To show the relevance of this system, a scenario involving joint and coalition forces is developed. The scenario demonstrates the usefulness and need for platform independent planning and analysis systems. Finally, this thesis recommends an architecture that USSOCOM should investigate for its future mission planning, analysis, rehearsal, and execution (MPARE) system.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of this thesis is to assist the United States Special Operations Command (USSOCOM) in the development of a planning and analysis system that meets their unique needs. Special Operations Forces (SOF) currently operate in a manner that is described by Joint Vision 2010 as the Armed Forces of the future. That is, a force that conducts joint service, multi-national, and interagency missions. These heterogeneous forces are also dispersed throughout a large area of operations. Additionally, SOF missions often involve unpredictable situations and are time sensitive in nature. Finally, Special Operation Forces operate throughout the operations continuum. Their missions can range from humanitarian assistance operations during peacetime to surgical strikes during a full-scale war. Therefore, a successful SOF planning and analysis system must be platform independent, distributed, flexible and extensible.

This thesis designed and partially implemented a platform independent mission planning and analysis system for the United States Special Operations Command (USSOCOM). The ability to move to platform independent technologies is particularly important for the special operations community since it can not expect standardized computer planning and analysis systems for their joint, multi-national, and inter-agency operations. This thesis also investigates the ability to integrate legacy systems using an open architecture on an object web. In addition, this thesis incorporates operations research methods into this system to show their importance in planning and analysis.

The system is developed in the Java programming language using a loosely coupled components architecture. This architecture allows military planners to incorporate only the components desired for a particular situation. This creates a system that is flexible and extensible. This particular system involves an image component that contains a map with overlays and a network algorithm component. The use of common object request broker architecture (CORBA) for integrating legacy systems is also discussed.

To show the relevance of this system, a scenario involving joint and coalition forces is developed. The scenario demonstrates the usefulness and need for platform independent planning and analysis systems. Finally, this thesis recommends an architecture that USSOCOM should investigate for its future mission planning, analysis, rehearsal, and execution (MPARE) system.

ACKNOWLEDGEMENT

I would like to thank Professor Gordon H. Bradley for his patience and genuine dedication to seeing me complete this project. It was only through his unparalleled commitment to the education process that I was able to finish this vaunted task. I would also like to thank LTC Charles Shaw who got me involved in this topic initially. He has an uncanny ability to insert NPS students into even the most major projects at the highest level of command. I also need to acknowledge the contributions of the "Loosely Coupled Components" research group. These include the master architect and head programmer, Professor Arnie Buss. He wrote the code for this system during a very condensed time period. Other members with significant contributions were MAJ Jack Jackson of TRAC Monterey and MAJ Arent Arntzen of Norway.

I also want to thank the officers of the USSOCOM, J7-C, namely COL Nolen Bivens and LTC Joel Parker who arranged for and sponsored my experience tour. I only hope they feel their investment was justly rewarded. I need to thank LTC John "The Man" Olshefski, John Cox (the father of MPARE), MAJ Steve Meddaw, LTC Marc Alderman, and Juergin Beuring for ensuring my time at MacDill was worthwhile.

Finally, and most importantly, I need to thank my wife. She carried our first child during this entire thesis process and never complained. I would never have finished this without her love and understanding. Thank-you dear!

I. INTRODUCTION

"Joint Vision 2010 provides an operationally based template for the evolution of the Armed Forces for a challenging and uncertain future. It must become a benchmark for Service and Unified Command visions."
John M. Shalikashvili
Former Chairman of the Joint Chiefs of Staff

Joint Vision 2010 [1] foresees the Armed Forces comprised of high quality people and information-age technologies. Empowered by these new technologies, future forces will be able to dominate their enemies across the full spectrum of military operations. The anticipated improvements in command, control and intelligence brought on by information-age technologies are significant and will transform current operational concepts. The traditional functions of maneuver, strike, protection, and logistics will change to a new conceptual framework of dominant maneuver, precision engagement, full dimensional protection, and focused logistics. The application of these four concepts, which leverage technological advances in command, control, communications, computers, and intelligence (C4I) systems, will provide the envisioned full spectrum dominance [1]. In effect, the future doctrine of our Armed Forces is predicated on advancements in information technologies, particularly those that improve command, control, and intelligence.

Other dynamic changes in military operations forecast by Joint Vision 2010 include enhanced jointness and even more multinational or combined operations. Future commanders will be expected to win all engagements in a more efficient manner [1]. This can only happen through "seamless integration [1]" of the Services' capabilities. The

Armed Forces of tomorrow are to be "fully joint: institutionally, organizationally, intellectually," and perhaps most important, "technically [1]." In addition, future operations will be more than just joint. The Armed Forces of 2010 will be expected to work together with allied and coalition forces [1]. These anticipated changes imply that prospective C4I systems must integrate across Service and multinational lines.

The final change identified by Joint Vision 2010 addresses the emerging potential adversaries. According to Joint Vision 2010, the U.S. must be prepared for a broader range of potential enemies. These probable opponents will be unpredictable in nature; but, we expect them to have many of the same information-age technological capabilities whether internally developed, purchased on the international market, or stolen. This requires future C4I systems to be intensely concerned with security.

The C4I systems of 2010 are in development today. They need to be, since these systems are the driving force of tomorrow's doctrine. These systems are being developed at the Joint level, each Service level, and throughout many of the Unified Commands. These systems seek to meet the goals set forth in Joint Vision 2010.

This thesis investigates the development of a new system for the United States Special Operations Command (USSOCOM). Since command, control, communications, computers and intelligence encompass such wide areas, this thesis will concentrate only on the mission planning and analysis portion of such a system.

A. BACKGROUND

1. Vision.

The United States Special Operations Command (USSOCOM) has its own vision of the future. This document is called SOF (Special Operations Forces) Vision 2020 and addresses the same issues identified in Joint Vision 2010. SOF Vision 2020 identifies the two fundamental strengths of Special Operations Forces as "quality people with unequaled skills and a broad-based technological edge [2]." This document further states that the defining characteristics of Special Operations Forces are that they are "sized, trained, and equipped to engage across the technological and operational continuums [2];" they are "regionally focused [2]", including cultural, linguistic, and political aspects; they are "rapidly deployable, surgical strike capable, and able to achieve combat, mobility, and information dominance on a limited scale [2];" and finally, they are "flexible and agile joint forces which can develop and execute unconventional, audacious, high pay-off courses of action [2]." These characteristics, which define the current and future state of Special Operation Forces, correspond with Joint Vision 2010's reliance on joint, multinational, mobile, and highly technical operations that will have dominance throughout the full spectrum of the operational continuum of the future [1]. This thesis does not seek to prove that the Joint Staff's vision of the Armed Forces of the future is similar to the Special Operation Forces of present; that appears to be evident. These defining characteristics were addressed simply to highlight that the same requirements placed upon a C4I system of the future by Joint Vision 2010 are even more germane for the Special

Operations community. Additionally, it is highly plausible that any system developed for USSOCOM could have an even larger group of users in the future.

2. Need

The best way to illustrate the Special Operations Forces' unique mission planning, analysis, rehearsal, and execution requirements is to first study their operations. An illustrative example of a Special Operation's mission that is joint, multinational, and even inter-agency is a strike mission. The operational plan (OPLAN) could have Navy SEALs actually striking a target. The SEAL team, being a small unit, could be supported by a conventional host nation coalition and that could block roads or other networks coming into the area, thereby isolating the target. The coalition host nation forces, generally not familiar with U.S. operations and often non-English speaking, could be supported by U.S. Army Special Forces (SF) who speak their language and provide liaison and communications. All of these units could be flown to the target area by U.S. Air Force and U.S. Army Special Operations aviation elements using fixed wing aircraft or helicopters. The intelligence products on the target include satellite photos, electronic or signal profiles, and even human intelligence and could be obtained from U.S. national strategic assets. The entire mission could be directed by the Theater Commander in Chief (CINC) in support of a National Command Authority (NCA) objective.

A mission this diverse requires a great deal of intricate planning, real-time analysis, rehearsal, and synchronized execution. Each unit has peculiar planning and analysis issues. For example, the SEALs will be concerned with the tides/sea conditions and enemy

dispositions; the SF will need to know what kind of weapons and communications the coalition forces use; and the aviators will be concerned with winds, landing zones, air defense threats, and other flight conditions. Each unit will analyze the situation and prepare their particular plan; however, all of these plans must also be synchronized and developed into one effort focused on the CINC's or operational commander's vision. This synchronization requires much coordination and collaboration. In order to accomplish this effort successfully, time critical planning and analysis must be done vertically from higher command to lower, such as from an operational Special Operations Command (SOC) to a Joint Special Operations Task Force (JOSTF), and horizontally among all units at the same level, such as from a SEAL team to a Special Operations Aviation Detachment (SOAD). Each unit will also want real-time intelligence of the enemy and target area simultaneously across various locations. A final concern is the distribution of forces. The SEALs could be on board a ship, the SF already in country, and the Air Force miles away at an air base in a third country. Special Operations' missions such as this require real-time, highly dynamic, distributed planning.

3. MPARE

The United States Special Operations Command is attempting to address these concerns. USSOCOM has approved a program called Mission Planning, Analysis, Rehearsal, and Execution (MPARE) which is currently at milestone 0. The Concepts Requirements Document (CRD) will be published this year.

The goal of MPARE, according to the Mission Need Statement dated February 24, 1997, is to provide:

> ...the architecture, masterplan and oversight to integrate disparate special operations-specific mission planning and execution systems, simulations and simulators and to ensure connectivity with relevant command, control, communications, computers and intelligence (C4I) networks. ...The key is to provide a coherent architecture that will allow all current and projected systems to exchange information in a seamless, automated fashion. Although integration of current and near-term systems must be addressed, the strength of MPARE will reside in its ability to develop a road map of the future which migrates existing systems into an architecture while providing a masterplan for future acquisition programs that is both financially prudent and operationally effective against tomorrow's threat.

Currently, there are several automated and computerized planning systems in USSOCOM. Some of these systems display digital maps with overlays, read and write to databases, and automate the orders process. Some are portable, PC based systems, and some run on network or standalone workstations. The operating systems (OS) vary and include Windows 95, Windows NT, Sun Solaris, or even proprietary OS. The near term goal of USSOCOM is to integrate these systems and then link them to models, simulations, simulators, and other analytic tools. USSOCOM's long term goal is to develop an architecture that will allow integration of individual mission planning systems operating on a variety of hardware platforms using differing software through a network. This feature will allow users to evaluate alternative plans through a simulation and analyze the results, feed the planning information to flight and ground simulators and rehearse the plan, and

finally continue feeding the special operator with real-time information during mission execution. Real time analysis using new data received during execution is also possible.

The SEALs on a ship, the SF in country, and the Air Force at an air base would receive the mission simultaneously from higher command. The units would then conduct vertical and horizontal planning while exchanging information over a secure network and continually receiving up-to-date, real-time intelligence on the enemy and the target. The plan would be integrated and approved by higher command. The higher command would send the plan back to a simulation center where it could be simulated and the results analyzed. Changes would be made and disseminated to the dispersed units synchronizing their efforts in real-time. The Air Force would feed the terrain and weather data into their flight simulators located at the air base and practice flying the mission. The SEALs would do the same in a ground simulator located on board ship while all units continue to receive intelligence updates from the SF located in-country and from national intelligence organizations (CIA, DIA). During the execution of the mission, all of the units would receive and send information to their higher command. The flow of information and continuing analysis of situations would not stop until the mission was successfully completed.

4. Problem

USSOCOM currently has a multitude of diverse planning systems that operate on different hardware platforms with different operating systems that are not interoperable. It is unreasonable to expect joint forces to discard existing legacy systems worth millions of

dollars and move to a standardized planning system on a common platform. The Services all have different planning and analysis issues that require different capabilities. The problem becomes even more challenging when dealing with other government or non-government agencies or even other nations. Additionally, these heterogeneous operating forces (joint, multinational, and inter-agency) are often dispersed and not able to gather for a detailed planning process or rehearsal. Compounding this situation is the unpredictable, time-sensitive nature of special operations. In addition, existing Operations Research (OR) analytical tools are not truly integrated into these current planning and analysis systems. Traditional OR models must be modified to allow easy input of data and quick analysis. The OR models must have a fast turn-around time in order to be useful. The solution for integrating such diverse planning systems, distributing them to dispersed operators, responding to unanticipated situations, and integrating analytical tools must involve an architecture that is truly hardware platform and operating system/software independent, extensible, flexible and able to leverage legacy systems and applications. This problem is not small or trivial to solve.

B. STATEMENT OF THESIS

The technologies to support the above-mentioned solution either currently exist or are emerging. These technologies provide the needed capabilities that can meet the unique demands of special operations. The missing element is architecture. This architecture must bridge the systems architecture that currently exists for numerous monolithic computer hardware and operating systems with the operational architecture based on the

standard operating procedure of the warrior. This bridging architecture between the hardware/systems architectures and operational architectures is currently being called a Joint Technical Architecture (JTA). Examples of current research in JTAs are the High Level Architecture (HLA), Distributed Integrated Systems (DIS), or other "middlewares." This thesis describes another part of this technical architecture that incorporates these new technologies to achieve SOF mission planning needs. The research constructed a proof-of-concept system to demonstrate some of these capabilities and to validate this technical architecture.

The technical architecture that this thesis espouses is platform independent, extensible, and network based. This is a truly open architecture that can support the addition of a number of components thus allowing a planning system to grow as needed. It can also leverage legacy systems. Additionally, this architecture is based on commercial-off-the-shelf (COTS) technologies that are inexpensive and widely available.

The proof-of-concept of this architecture is a technical demonstration of a map-based planning and analysis system. This system was developed in a short time using this open architecture. This digital map-based planning and analysis system is a truly platform independent system using the COTS technologies of Java. It is also network based, giving it the ability to retrieve and distribute information to dispersed units. In addition, the system incorporates Operations Research analytical models.

A special operations scenario is developed in order to show the applicability and capabilities of this planning system. This scenario involves the integration of joint,

interagency, and multinational forces. It also demonstrates the need for OR tools. This scenario is fictitious, thus allowing the thesis to remain unclassified.

The goals of this research are to demonstrate a platform independent, extensible, interoperable planning system. The research also shows the importance of OR in the planning process. Finally, it provides USSOCOM with some insights into developing their MPARE system.

This thesis consists of five chapters and two appendices. Chapter II defines some concepts that are key to understanding the rest of the thesis. Chapter III describes the related research in this field and will cover many of the Joint and Service peculiar systems currently being developed. Chapter IV details the design of the system developed for this thesis; it first reviews the USSOCOM planning requirements, then discusses the system structure. Chapter IV also includes the overall architecture as well as the particulars of the system built for the technical demonstration. The capabilities shown in the proof-of-concept are discussed next. This discussion is followed by a description of the system capabilities that are not implemented in the technical demonstration. Chapter V discusses the security of such systems and covers the dangers that are inherent in these systems and some possible resolutions. Chapter VI offers conclusions and includes recommendations for the future development of such systems. Appendix A is an explanation of the scenario used to demonstrate the capabilities of the system. Appendix B provides a walk-through of the system through the use of captured screen shots.

II. KEY CONCEPTS

Before proceeding further, some vital concepts are defined. These items are associated with network computing and object oriented programming which are part of the bedrock of this thesis.

Platform independent - the concept that a particular software program can run without modification on different computer hardware running different operating systems. For example, a platform independent program can work without change on a personal computer (PC) running Windows 95 or a Hewlett-Packard workstation running UNIX.

Java – a programming language originally developed by Sun Microsystems for small electronic devices. This language is small and platform independent. Unlike other programming languages like C++, which compile their code into machine code optimized only for a PowerPC or a Pentium, Java source code translates into Java byte code that is not designed for any machine in particular. The Java byte code can run on any machine that is configured as a Java virtual machine (JVM). The JVM is a virtual model of the computer's Central Processing Unit (CPU). This frees programmers to write code that can run not only on popular PCs but also on other machines ranging from large super computers to small hand-held devices.

Component – a section of software that performs a task. A software component has a well-defined interface and is able to be distributed to other applications. An example of a component may be an algorithm that solves a simple problem. The code for this

algorithm will have a well-defined interface that allows other programmers to take the algorithm code and use it in their particular program.

CORBA – the Common Object Request Broker Architecture [19]. A middleware developed by the Object Management Group (OMG), which is a consortium of over 700 computer industry companies (minus Microsoft). This computer architecture allows interoperability of components executing on different computers. This allows components written in different programming languages, running on different operating systems to work together.

Object Web – an integration of the CORBA components or distributed objects and the World Wide Web [19]. CORBA protocols are the common way to connect these components on the Internet.

" the network is the computer" – the idea espoused by Sun Microsystems. Unlike the past, all the work need not be done by one machine. The user can distribute his work and access information across several computers on the network.

"loosely coupled components" – a computing architecture researched by G.H. Bradley and A.H. Buss at the Naval Postgraduate School [3]. The basic precept is that systems can be constructed quickly and inexpensively by bringing together various components. The components can be accessed anywhere and are designed so that they link to a system like a "Lego" block. Only the components needed by the user are fitted into the newly developed system. The system can change to meet the user's need because the components are "loosely coupled" and can be easily added or dropped.

Object Oriented – this is a programming style that concentrates its design on the data, or objects [18]. This programming style consists of small classes and methods that perform a set of tasks. These small objects are then pieced together to accomplish a larger task. This concept is different from older procedural programming where everything was done in a step method. A good analogy is to think of the construction of a computer [18] from standard components such as memory chips and the central processing unit that are manufactured by different companies and can be put together to build a computer. C++, Smalltalk, and Java are examples of Object Oriented programming languages.

III. RELATED RESEARCH

"The Warrior needs a fused, real-time, true picture of the battlespace and the ability to order, respond and coordinate vertically and horizontally to the degree necessary to prosecute the mission in that battlespace."

Joint Pub 6-0

The explosion of information age technologies has inspired an increased interest in the development of military command and control systems. The Department of Defense (DoD) embraced these new technologies with the formation of the Defense Information Systems Agency (DISA). This organization has led the way in the DoD's development of joint command and control systems. Additionally, each Service has conducted research and developed test systems at their level. This thesis will discuss DoD level research, Service component research, and finally research being done within the U.S. Special Operations Command.

A. DEPARTMENT OF DEFENSE RESEARCH

The mission of DISA is "to plan, engineer, develop, test, manage programs, acquire, implement, operate, and maintain information systems for C4I (Command, Control, Computers, Communications and Intelligence) and mission support under all conditions of peace and war" [4]. Most importantly, DISA is the manager of the Defense Information Infrastructure (DII) [4]. The Defense Information Infrastructure attempts to integrate all DoD communication networks in order to pass information on to the warfighter. The main elements of DII are the Defense Information System Network

(DISN), the Defense Message System (DMS), the Global Command and Control System (GCCS), and the Global Combat Support System (GCSS) [4].

The Global Command and Control System (GCCS) provides integration of the different command and control systems of DoD and the Services. Its infrastructure is made up of UNIX based server and personal computer terminal workstations. These units are connected by the Secret Internet Protocol Router Network (SIPRNET), which is the secret level of the DISN [4]. The GCCS "system of systems" architecture consists of two parts. The first is a set of related databases and the second is applications, both of which are accessed through servers [5]. One of the application servers acts as the executive manager (EM) which offers desktop services and is used as the user interface [5]. The applications are in two groups. The first group is the Common Operating Environment (COE) and the second group is Mission applications [5].

The Defense Information Infrastructure-Common Operating Environment (DII-COE) establishes a set of standards for "common support applications and platform services" which are needed by the different mission applications [5]. These mission applications include the Joint Operation Planning and Execution System (JOPES) – a command and control system currently used to plan joint military operations [5]; the Evacuation System (EVAC) – a U.S. State Department system that tracks U.S. citizens outside the United States [5]; and the Joint Deployable Intelligence Support System (JDISS)- a link to numerous military intelligence sources [5]. The concept of DII-COE calls for the military planner to pick the applications he needs for the mission. The support

applications that are common to those mission applications are then made into a subset or variant for this particular mission. This Common Operating Environment-Variant (COE-V) would allow the different systems to interact with each other [5].

DISA has also established standards for data. These standard databases are essential for the successful use of GCCS. DISA made over 1200 data standards which were based on JOPES applications [5].

GCCS and the other elements of the DII are all currently being evaluated by the Joint Interoperability Test Command (JITC) located in Fort Huachuca, Arizona [6]. As the major field operating activity of DISA, JITC provides testing for private industry, federal agencies, US and allied military services and the regional CINCs [6]. JITC also certifies all Joint systems used throughout the DoD.

DISA's research is important to this thesis because it offers the current standard that all systems must achieve. Also, any system fielded by USSOCOM would have to be evaluated and certified by JITC. Finally, the concept of integrating legacy mission applications is one of the goals of this thesis.

B. SERVICE COMPONENT RESEARCH

Each Service component is working their individual piece of the Global Command and Control System (GCCS), as well as their own Service peculiar systems.

1. Army

The U.S. Army's vision of the future is encapsulated in their Force XXI process. The Army has established Joint Venture, which is their reorganization of the Tactical Army [7]. They have set up the Army Digitization Office and numerous battle labs to develop future concepts and to test technologies[7]. The 4th Infantry Division (Mechanized) has been redesigned as the "Experimentation Force" or EXFOR. The EXFOR has conducted numerous Advanced Warfighting Experiments (AWE) to test new information-age technologies. These AWEs have been conducted at the platoon, company, battalion, brigade and even division level.

The systems being tested by the Army are too numerous to be mentioned here, but one of particular interest to this thesis is the Maneuver Control System (MCS). The MCS is designed to replace map boards and overlays and to give commanders a picture of the battlefield on the computer using an interactive interface [8]. This will allow information to be distributed quickly to all levels.

2. Air Force

The U.S. Air Force Information Warfare Center has the task of digitizing the air battlespace. Through documents like the Global Engagement: A Vision for the 21st Century Air Force, they have started programs to study future command and control systems. The Air Force calls these Battle Management/Command and Control (BM/C2) systems. The concept of these systems is the same as the Army's, which is to provide

future joint commanders with real-time information allowing them to control and execute all air and space missions [9].

3. Navy

The U.S. Navy has approached the future with equal vigor. They have established the Fleet Information Warfare Center and have conducted Fleet Battle Experiments (FBE). The Navy has also taken steps to standardize their information technologies (IT) with IT-21. IT-21 will move all of their computer systems to Windows NT operating systems. This is important because the system designed here will have to work with Windows NT.

Other Navy research projects of interest to this thesis are the Tactical Decision Making Under Stress (TADMUS) program which is sponsored by the Office of Naval Research. This is a system that integrates command and control information and attempts to aid in the decision making process. This system displays map-based information needed by the naval commander. Another system of interest is the Enhanced Common Operational Picture (ECOP) which is a map-based system, written in Java, that displays information with overlays [10].

4. Marines

The U.S. Marine Corps is working closely with the Navy and its systems; but, they are also testing a system of particular interest to this thesis. Stanford Research Institute (SRI) International, a private company, has developed a system called InCON® [11]. SRI claims it is a "wireless, portable information management system" [11]. It is map-based,

written in Java, and runs with a CORBA server. It is also platform independent. The Marines are testing this system through their URBAN Warrior concept.

This system is of interest to this work because it has a similar design and architecture. It takes advantage of Java's platform independence and Common Object Request Broker Architecture's interoperability.

C. USSOCOM RESEARCH

There are several current research projects within the U.S. Special Operations Command. The Common Operational Modeling, Planning, and Simulation Strategy (COMPASS), which is actually sponsored by the Defense Modeling and Simulation Office (DMSO), is an attempt to bring distributed planning and modeling and simulation together. The COMPASS system interacts with command and control systems by shared "geo-registered and pixel-based" data [12]. It is map-based and allows the transfer of messages from various commands through video teleconferencing (VTC). This system was tested during Roving Sands 97 (the annual Joint Operations Interoperability exercise conducted by JITC after nomination by USSOCOM) [13].

Another system of interest is the Information Operations Planning Tool (IOPT) being developed by USSOCOM (J-2) [14]. This is a system that integrates intelligence and other information needed for planning. It is of interest because it is written in Java and will run with a CORBA server.

The final system of interest is the Special Operations Forces Planning (SOFPLAN) being developed by BBN corporation for the Joint Special Operations Command (JSOC) [15]. This system is written in Java and designed for laptop PCs using a Local Area Network (LAN) or airborne assets [15]. The SOFPLAN creates a visual Synchronization Matrix that allows the planner to integrate several players on the same timeline. The system then translates the Synchronization Matrix to an Execution Checklist which allows the commander to track events as they happen.

The research being conducted by members of USSOCOM, the Service components, and DISA are all designed to help the warfighter. The systems developed have common themes of interoperability, distributed networks, and map-based data references. The system developed in this thesis is based on the same characteristics.

IV. DESIGN

> *"Operations research is a scientific method of providing executive departments with a quantitative basis for decisions regarding the operations under their control."*
> **Morse and Kimball [16]**

New technological capabilities have enabled the design of an open technical architecture that will meet the requirements of USSOCOM. A review of these requirements is followed by a description of this architecture and overall system structure. A planning and analysis system has been constructed for this thesis as a proof-of-concept. This system serves as a technical demonstration of the overall system's capabilities and helps validate the open architecture. This proof-of-concept is focused in scope, simple in nature and certainly does not demonstrate the total potential of these new technologies and the architecture. This chapter ends with a detailed discussion of the system's potential to include capabilities not implemented by the technical demonstration.

A. SYSTEM REQUIREMENTS

This system was designed to meet the particular requirements of USSOCOM. The entire future Armed Forces, not just Special Operations Forces, will need similar systems. The system's requirements include the capabilities to: run on any computer hardware, be distributed to actors at all planning levels, and be flexible enough to change for each situation (including unanticipated situations). In addition, this system should be extensible. The planning and analysis system's technical architecture should be capable of extending itself to run simulations, incorporate OR tools and other forms of analysis. This

would allow such a system to be the cornerstone of the MPARE concept. Finally, the system should include the information management capabilities that make automated systems so valuable.

B. TECHNICAL ARCHITECTURE

1. Loosely Coupled Components

The architecture for this system is based on the use of "Loosely Coupled Components" championed by Dr. G.H. Bradley and Dr. A.H. Buss, both of the Naval Postgraduate School [3]. This architecture builds planning systems by integrating various components as required in a highly flexible manner. Examples of these components include maps, situational overlays, analytic algorithms, or any other tasks needed for the system's proper functionality. The planner assembles these separate components to build a system that meets his immediate needs. This concept of flexible system construction is different than most systems built at the larger application level. By building systems from the smaller component level, planners are afforded systems that are more flexible, extensible, and responsive.

2. Component Interface

These components may be located anywhere on a computer network. This network may be the SIPRNET, a Global net, or an intranet established for a particular mission. The planner either establishes links to these components remotely or downloads them onto a computer. The fundamental element in this system is the component interfaces. Each component has an interface that explains what the component does and

how the component is activated. The planner does not know and does not need to know how the component works internally. This same interface will also contain a standard protocol that will enable different components to communicate. Two types of interfaces for component algorithms are described in [3]. These include the local execution interface – where the algorithm is downloaded over the network and executed on the planner's computer using the data stored locally; and the remote execution interface – where the algorithm reads the data over the network from the planner's computer and sends a solution back [3]

3. Network-Based Technologies

This architecture makes full use of the network and new network-based technologies. The planning and analysis system can be built by components accessed over the global web/object web. The data, maps, algorithms needed by planners can also be retrieved or distributed via a network. An essential tool in this network-based architecture is the Java programming language. This language is perfect for systems that may have different computer platforms integrated on a network. Components that are written in Java will be able to operate anywhere. This will make such components easier to download onto a planner's system and easier to distribute to other computers.

This architecture does not require all components to be written in the Java programming language. Components not written in Java may be accessed and distributed by the Common Object Request Broker Architecture (CORBA). CORBA develops a common interface among different languages and allows components to become

distributed objects on a network. This will allow parts of legacy applications on systems written in other programming languages to be integrated into new systems.

The combination of the new technologies of Java and CORBA make this architecture extremely powerful. New systems can be built from components retrieved from anywhere on a web. These components can be written in Java and accessed with a local execution interface or written in another language and used with a remote execution interface. The components could be new or parts of legacy applications on systems that are accessed through CORBA. The new technologies inherent in this architecture create a flexible, distributed, extensible system that can leverage legacy systems and meet the specific needs of the planner.

C. DEMONSTRATED CAPABILITIES

A simple planning and analysis system was developed as a proof-of-concept of the architecture described in this thesis. The system is designed to distribute planning elements to different hardware platforms through a network. The planning system displays a map of the operational area. The map is simply brought into the system and the planning and analysis system then allows overlays to be added to this map. These overlays can be of the enemy situation, friendly situation, or any other element of information needed for the mission. The system also has the ability to manipulate the display. The map can be faded or dissolved to better display the overlays and other information entities. Finally, to illustrate the architecture and the importance of OR in planning, this planning system reads a graph from the display and executes a shortest path algorithm. This entire

planning and analysis system is comprised of several integrated individual components. A further explanation of this system is included in Appendix B.

This simple, austere system was designed to demonstrate new technological capabilities and validate the architecture. These capabilities stem from both the programming language and the architecture.

1. Platform Independent

This program is written in a recent version of Java. In previous versions of Java, the Alternative Window Toolkit (AWT) created all of the Graphic User Interface (GUI) elements. This AWT yielded a GUI that worked correctly, but looked different on different operating systems. The new version of Java, with a new GUI package called "Swing", creates a GUI that looks the same on all operating systems. In other words, the system will have the same look running on an Apple PowerBook G3 as it will on a Compaq running Windows NT.

The benefits of platform independence are enormous. First of all, designing a system for a particular computer chip is risky. The growth in technology is so fast that a powerful computer today may be a good doorstop two years from now. Additionally, it is unreasonable to assume that all the diverse players involved in a special operations mission would be using the same hardware or even operating system. Moving all services to computers and one operating system, like the U.S. Navy is doing with IT-21 (moving everyone to Intel-chips running Windows NT), may be the solution for a particular service; but, this would be difficult to support outside of that particular service. It is not

realistic to expect the Army, Air Force, CIA, State Department, Red Cross, Doctors without Borders, UN, and every country SOF will ever work with to move to one common platform.

A final benefit of platform independence is one described by T.R. Halfhill in BYTE magazine [17]:

> A virtual platform such as Java is cross-platform not only in the horizontal dimension, but also in the temporal dimension. No matter what new platforms appear, only the JVM [Java Virtual Machine] and native compilers will have to be ported-not the applications.

This has significant implications for the military. The millions of lines of code in use by the military today would have to be rewritten or changed, recompiled, cross-compiled and ported for more advanced computer systems if traditional methods are used. The programs that run on a PC or a laptop today may need to run on a cell phone or small hand-held device in the future. The ever-evolving computer technology gives little clue as to what will be the ideal computer in the military of the future. Regardless, unlike programs written in other programming languages, programs written in Java would not have to be rewritten to fit the new computer. Only the JVM would have to be configured for each new piece of hardware.

2. Distributed

The planning and analysis system has the capability to distribute through a web to several dispersed operators. The Java programming language makes this distribution possible. Java has been called the "language of the Internet" because it has the ability to open and access objects and files across a network. Java also has a large library of

routines to deal with the protocols of the Internet [18]. Combining the network capabilities of Java with a CORBA client/server allows access to information or objects from other systems. This allows the user to pull information from various sources on the network. This system can read maps and situational overlays from files located on the local hard drive or somewhere else on the network.

A distributed planning and analysis system is very advantageous. Information can be pushed down to operators or pulled by the operator. For example, a map of the area of operations, used as a basis for the planning, could be accessed over the network and then distributed to all planners involved with the particular mission. In addition, other maps or intelligence products could be obtained and distributed. The intelligence information of the enemy situation could be accessed from a database and sent to another unit located miles away. Additionally, mission orders could be issued through the distributed system. This would relieve the commander of the often impossible task of collecting a heterogeneous, dispersed force together for a planning session.

3. Extensible

The system is extensible because of both the Java language and the "loosely coupled components" architecture. Java is an object oriented programming language and as such its tasks are done by objects or components. The systems architecture integrates these components. The components may work together or they may work alone [3]. The components have their own individual task that is different than the other components. The premise of this architecture is that the inner workings of these components is not

important to the user, only the way the component interfaces is important. These components can be obtained from anywhere and pieced together to build the system needed.

In the demonstration proof-of-concept, the components are the map component, the overlay components, and the network algorithm component. These components could have been pieced together anywhere. An analyst could have built this planning and analysis system by knowing what components were needed for this particular mission and how these individual components interacted with each other.

This extensible system has great advantages. First of all, it is flexible. The components can be added or dropped from the system as needed. This allows the system to be dynamic. It can change for different situations. For this planning and analysis system, the scenario calls for a network interdiction. The shortest-path algorithm component was added to this system because it proves valuable to the military planner for this scenario. This flexibility increases when the components are accessed over the network.

The web also provides an additional advantage for this extensible system. Only the components needed would be accessed over the network. This creates the "thin client". The user only retrieves the data and applications needed to accomplish the mission. This keeps his computer free of excess data and information. This "thin client." is especially appropriate for small, hand-held computers that might be used by SOF. By having the ability to access only the components needed, the operator's small computer has all the capability of the network's computers.

Another benefit of extensibility, is the ability to reuse components [3]. This allows components to be shared among various military planning systems. Rather than running an entire program just to get to the one capability needed, the components of one system can be taken out and embedded in another system. This is similar to building a custom stereo system from separate standard components. A CD player or speakers from one system can be added to another by simply installing the one component, not the entire system. This concept will lead to a decrease in large, expensive planning and analysis systems and an increase in smaller, more efficient, flexible components.

4. OR Tools Integrated

The integration of OR tools is made possible by the system's extensibility. The friendly, enemy, and road network overlays are read in as a graph. A shortest path algorithm is added as a component. This algorithm reads the data from the graph and finds the shortest path from each enemy location to the objective. This information is helpful to a planner who wants to know which enemy position poses the greatest threat. This OR tool was added to demonstrate the loosely coupled components extensible architecture, moreover it shows the importance of OR tools in the planning process. These analytical tools are usually left out of planning systems because they are too difficult to integrate, too complex for the user to implement, or too slow to be useful for military operations. This architecture allows analysts and planners to integrate OR analytical tools when they are needed, creating a planning and analysis system. These tools are components that can be accessed to meet the immediate needs of the particular mission. This can be done at several levels throughout the planning process, thereby allowing more

planners, analysts, and operators to take advantage of the powerful capabilities of Operations Research analytical tools.

5. Security

This planning and analysis system demonstrates just one simple way to transmit data securely. A software steganography program was used to show how data could be transferred. Steganography is the technique of concealing files in some other form of data. This program allows files, such as the enemy situation, to be concealed in computer picture files. This technique will be discussed more fully in the next chapter.

6. COTS

This system was developed entirely with software and hardware that is Commercial-off-the-Shelf technology. These technologies are both widely available and relatively inexpensive. This allows for systems that are easy to develop and distribute.

D. SYSTEM POTENTIAL

Due to time constraints, this proof-of-concept was not able to technically demonstrate all the potential capabilities of a system such as this. The features already demonstrated should prove extremely valuable to USSOCOM, military planners, and analysts in general; however, there is the possibility of even more benefits. None of the potential capabilities of this system described below are inconsistent with the present architecture.

1. Object Web and Legacy Systems

There are several planning systems that are currently being used in USSOCOM. The SEALs have the Special Warfare Mission Planning System (SWAMPS), the Air Force has the Special Operation Forces Planning and Rehearsal System (SOFPARS) which consists of a UNIX based Mission Planning System (MPS) and a PC based Portable Flight Planning System (PFPS) using Falconview. The Army has Maneuver Control System (MCS) which is an offshoot of GCCS. Currently, the CORBA can leverage some aspects of each of these systems. CORBA takes the components or distributed objects from these systems and allows them to interact and discover each other [19]. Most of the success in this area has been the access and distribution of data. The distribution of certain types of images and other more complex components is more difficult and has not yet been accomplished successfully. This is a functionality of CORBA that requires more research.

The interfaces needed to get the components together are defined by the component's Interface Definition Language (IDL). The IDL is an operating system and programming language independent interface that allows the programmer to interface with components in the computer language he is using. Currently there are IDLs for C, C++, Ada, Java, and Smalltalk (COBOL and Objective C are on the way)[19].

CORBA should be able to access some of the databases in the current inventory of USSOCOM planning systems. For example, if the Air Force has a good set of data on airfield drop-zones, which they do in Falconview, this component of their program could be distributed through a client/server relationship on an object web. The SEALs or the

Army could access this particular data and use it for their system. This is an exciting concept that is made possible by this architecture.

2. Collaboration

The Java language and CORBA servers could easily support collaborative planning. The information from one computer terminal could be sent to another. For example, a flight plan developed by the Air Force on one computer could be sent to their potential passengers who were located elsewhere on a network using a different computer system. This would allow the real-time vertical and horizontal planning needed for time-sensitive missions.

3. Simulation

The system could incorporate modeling and simulation into the planning process. The same information that helped develop the plan could translate into a simulation. The base map used as the centerpiece of this planning tool can be changed to a Digitized Terrain and Elevation Data (DTED) map. This would give greater detail on terrain and be more beneficial to the ground operators. Some level of DTED is needed for most simulations. The planning system could incorporate components that would extract the information needed to run a conventional, high-end simulation like JANUS or it could integrate a Monte Carlo component. Such a component would allow Monte Carlo simulation with little additional effort. The Monte Carlo model would be general enough that the interface would only want to know which parameters would need to be randomly

generated with which probability distributions using prescribed transformation methods. This would give the planner another OR analysis tool with which to evaluate the plan.

4. Security

Some conditions of security have been demonstrated and more will be discussed later; however, this system has security aspects that are worth mentioning here. The Java programming language was developed with a great deal of consideration for security [18]. A Java program cannot disrupt memory outside of its operating space and it cannot overrun its run time stack [18]. This makes Java programs far less vulnerable to viruses.

5. Miscellaneous Components

The extensibility and flexibility enabled by the system's design allow growth. This system can add components that would give it the different capabilities desired by diverse planners.

The planning system could incorporate OR analytical tools other than simulations or shortest path algorithms. These could include linear or non-linear programs as well as other statistical methods. This would be beneficial to the planner or analyst using the system.

The system could incorporate a better messaging procedure between dispersed users. This could be in the form of white-board messaging or Video Tele-Conferencing (VTC). The components that have this functionality would simply be added to the system.

Information management tools could be added to this system. These could include an operational order template which would speed up the writing of the operations order;

an intelligence folder which could hold photographs, blueprints, or other detailed data needed for planning; or briefing formats, which could allow planners to more easily brief their plan to operators or commanders. These information management tools could be added to this system easily, and would take advantage of the capabilities of automated systems.

The planning system developed for this thesis does not have sufficient capabilities to make it an operational system. Its value is in the validation of its architecture and demonstration of its technological capabilities. These reveal the true potential of the Java programming language, CORBA, and use of Loosely Coupled Components architecture to build planning and analysis systems. It is the potential of these systems that provides the most gain to USSOCOM and should provide significant help with the development of their MPARE program.

V. SECURITY

An underlying yet preeminent concern with such systems is security. Automated systems such as this suffer from two types of threats. They can be categorized as external and internal. External threats are those that harm the actual hardware of the system. These threats can come in different forms but their common link is the damage they do to the actual computer hardware. Internal threats are those that can harm the software or network of the system. These threats leave no physical mark; but, they do disrupt the inner workings of the computerized system. Both threats are probable in the foreseeable future and should be addressed in any credible study of this kind.

A. PROBABLE THREATS

Joint Vision 2010 states that the enemy of the future will come from a broad range of potential adversaries [1]. This is best illustrated by looking at the probable threats to information systems. The external threats to such systems come from large, expensive devices that can only be expected from technologically advanced states or state sponsored terrorists. The internal threats can come from a wide range of actors and are far more pervasive and ubiquitous. These threats are inexpensive, require little overhead, and can be fielded by advanced countries, terrorist groups, small groups, and even individual hackers with no large sponsorship. This wide range of threats makes security a vital issue.

1. External

External threats, or threats that damage the actual computer hardware, currently come from two major sources. The first is High-Altitude Electro-Magnetic Pulse (HEMP) [20]. The second is High Power Microwave [21].

a) HEMP

HEMP is a nuclear explosion at a high altitude. The explosion does no large structural damage and because of its height will not kill anyone. However, the explosion does produce a large Electro-Magnetic Pulse (EMP) which transmits a huge amount of electricity through the atmosphere. The descending electrical cloud sends EMP through all electrical systems within some effective radius based on the yield of the munitions. This creates an overload or surge of electricity that overheats circuits and destroys unprotected electrical equipment. Computer systems with sensitive circuits are particularly vulnerable. The threat of HEMP can only be expected from a small number of nuclear-capable enemies. The threat is somewhat improbable because of the enormous expense and risk; but, in a high-intensity conflict with a nuclear-capable enemy, HEMP could become a viable option.

b) High Powered Microwave

High Powered Microwave is similar to HEMP in that a large amount of electricity is directed toward sensitive automated equipment, but is directed by powerful microwaves instead. This is a highly sensitive, very classified topic area that requires no further discussion be undertaken in this paper. The probability of encountering such

weapons is quite limited due to the expense and very limited availability of these platforms. Regardless, systems still should be protected against such a threat.

2. Internal

Internal threats are much more likely and therefore more dangerous. These threats come in several forms. These include inserting false data or viruses into the systems, stealing valuable data or programs from the system, or manipulating the performance of the system [22]. Internal threats are a danger to civilian and military systems alike. Internal attacks of computer systems have occurred numerous times throughout the history of such systems. These attacks can come from sophisticated, well-sponsored units as well as from unaffiliated individuals. It is attacks of this form, on the inner workings of the system, that are the most probable, harder to detect, and strike the most fear in the operators of automated military planning systems.

B. POSSIBLE RESOLUTIONS

There is no certainty when trying to find resolutions to the security problems of information systems. The resolutions are more like coping strategies. This is a well-researched and well-financed field of study. This thesis will discuss only the resolutions that are applicable to military planning systems.

1. External

The best defense against the external threats of HEMP or High Powered Microwave is the hardening of computer systems. This would require that the hardware used for such systems would need to be protected by surrounding all components with

metal. These metal covers must completely encapsulate the hardware system [20]. This is a very expensive process, especially when considering the number of COTS systems that would need this protection. Another option is to keep replacement parts available. These parts would remain in a protected area until needed [20]. Both HEMP and High Powered Microwave attacks are short-lived. The damaged parts of the system could be replaced after the attack. This again is expensive. A detailed analysis must be done for each situation weighing the probability of attack versus the cost of protection.

2. Internal

Internal defense must be conducted without question. Again, these defenses are not perfect, but should provide enough protection to accomplish the mission. The threats of inserting viruses and manipulating the performance of the system are dealt with by limiting access to the system. Discretionary Access Control (DAC) policies are used to permit or deny users to access a system [23]. These policies include password schemes, permission bits, and access control lists [23]. Password schemes give a password to every file. This requires users to know the password for each file they want to access. This is a logistical nightmare; but, it makes it more difficult for hackers to access protected files. Permission bits assign read, write, and execute permission for each file to individuals and groups by placing particular bits before each file. This is also difficult to manage; but, it secures access to systems and is very difficult to crack. Capability lists are similar in that they assign owners of files and allow the owner to determine who has what capabilities (read, write, execute) for each file. These policies protect files and limit access to the

overall system. This makes such systems less vulnerable to viruses and less likely to fall out of the control of the proper users.

Systems such as this are vulnerable to malicious software [23]. This type of software, called a Trojan horse, performs one function openly, but secretly performs malicious functions. The best way to combat such software is to limit the amount of new software allowed on the system.

The threats of false data or stolen data can be combated by Cryptography and Steganography [23]. Cryptography is using encryption to encode messages and conceal text. This is an ancient military art and there are several encryption algorithms. The most popular forms of encryption for computer systems involve the use of public and private keys. Keys are cipher algorithms that use complex mathematical formulas to translate text into encoded text. Everyone with access to the internal network knows the public keys but only the individual knows his private key. The private keys are mathematically linked to the public keys. Ideally, all message traffic would be sent with private keys known only to both sender and receiver; however, this is too costly. The more times a key is used, the easier it is to decipher. This requires private keys generally be changed frequently and this is not an easy process. It requires a great deal of effort to get a new private key to both the sender and receiver on a frequent basis. To send a secret message with a public key, the sender encrypts the message with the receiver's public key. The receiver then decrypts the message with his private key. There is a problem with this system. Although the message is secret, since only the receiver has the private key, it is not guaranteed to come

from the correct sender. Everyone has access to the public key so that anyone could have sent the message; therefore, the message could be deceptive. If the sender encrypts the secret message in his own private key and the receiver decrypts the message with the sender's public key, the receiver is assured the message came from the correct sender, since he is the only one with the private key. However, since everyone on the network has access to the public key, in this case, the secrecy of the message is lost.

The solution for both authenticity and secrecy, without resorting to the overuse of private keys, is to use a mutually available hash function to encrypt and decrypt messages. The sender sends two messages, one encrypted by the receiver's public key and one encrypted by the hash function and then the sender's private key. The receiver then decrypts the sender's private key message with the sender's public key. He also uses his own private key to decrypt the message encrypted by his own public key. The receiver then takes this message and encrypts it with the mutually available hash function. The receiver then compares his hash function message with the sender's hash function message to see if they are the same. If they are, then the secret message must have come from the correct sender and is legitimate [22].

The Java programming language has a cryptography toolkit; called the Java Cryptography Extension (JCE), that makes a set of application programming interfaces (APIs) for advanced software encryption technologies. This is algorithm-neutral which allows any producer of cryptography software to integrate their systems easily with these APIs. This JCE has the public/private key agreement technology and allows the secure

transfer of data across platforms and across protocols. In addition to encrypting data and information, this toolkit also allows objects or components to be encrypted [25].

Steganography is another ancient military art revamped for the information age. This is the ability to hide messages in the context of other traffic. Steganography offers the capability of concealing files in other forms of data. Digital data is by far the easiest to use for hiding scanned images and sound samples [24]. The key here is the fact that the enemy is being fooled as to what is the true data being sent. Steganography takes the least significant bits from a scanned image or a sampled sound and replaces those bits with the data that is being hidden. Several types of algorithms systematically remove and replace these least significant bits, which distorts the picture or sound a little. However, the distortion is so small it is not noticeable. The enemy is fooled into believing that the scanned image or sound is the message being sent, when in reality the true message is hidden within. The receiver, with an appropriate password, can run the same algorithms to reveal the true message. This is a very effective way of sending messages secretively. Steganography combined with encryption is a very secure way of transmitting data on a network.

The security of any military system is an essential concern. This concern is even more vital when the system is computerized and subject to unusual and dangerous threats. There are no sure bet defenses against these threats; but, there are several coping strategies that alleviate much of the concern and allow automated, military systems to function well enough to accomplish the mission successfully with manageable risk.

VI. CONCLUSION

This thesis provides the architecture for development of a planning and analysis system that would meet the unique needs of USSOCOM. A viable system for special operations must be able to operate on any type of computer hardware, distributed to operators dispersed throughout the area of operations, and flexible enough to meet the unpredictable situations encountered during SOF missions. This architecture, based on the loosely coupled components idea and enabled by new network-based technologies, provides the required capabilities.

A proof-of-concept was constructed to technically demonstrate these capabilities. This demonstration involved the construction of a simple planning and analysis system that involved the integration of several components. This demonstration helped validate the architecture. This architecture also supported a planning and analysis system that integrated Operations Research analytical tools, addressed system security, and used widely available Commercial-Off-The-Shelf technologies.

Consistent with this system architecture is the use of Common Object Request Broker Architecture (CORBA) to leverage some aspects of legacy systems. In particular, the databases of such systems can be accessed. The interoperability of the systems overall is still being researched. This system could also allow collaboration among planners that were connected via a network. Another extension of this system, in total compliance with the architecture, is modeling and simulation capabilities.

Security of this system is a major issue and must be integrated fully into the design. The threats confronting automated systems in the information age are far ranging and very dangerous. Many strategies are available to help combat these threats.

The architecture and the proof-of-concept demonstration should provide a good basis for the future development of military planning and analysis systems. In particular, this thesis should give USSOCOM's MPARE program a good basis to build upon. The ideas of building an extensible system by integrating components and leveraging legacy systems are fundamental to meeting the needs of the MPARE system. Incorporating OR analytic tools such as those demonstrated is especially important. The system architecture developed in this thesis provides the foundation for a platform independent, distributed, extensible planning and analysis system that will meet the needs of the Special Operations Forces of today and potentially all of our Armed Forces of tomorrow.

APPENDIX A. OPERATIONAL SCENARIO

This special operations scenario was developed to illustrate the capabilities of the technical architecture and possible applications of the planning and analysis system. Even though this scenario appears to be based in actual operational areas, it is totally notional and should remain unclassified. This scenario is based on an area of operations in Bosnia. A Joint Special Operations Task Force (JSOTF) has been formed and is headquartered in Italy.

TASK ORGANIZATION - The JSOTF has the following forces:

1 x JSOTF Headquarters (HQ) fully staffed located at an airbase in Italy

1 x SEAL platoon aboard ship in the Adriatic

3 x Special Forces (SF) Coalition Support Teams in Bosnia.

3 x United Nations (UN) Peacekeeping Forces

1 x Special Operations Aviation Detachment (SOAD) located at an air base in Italy

The layout of forces is as follows:

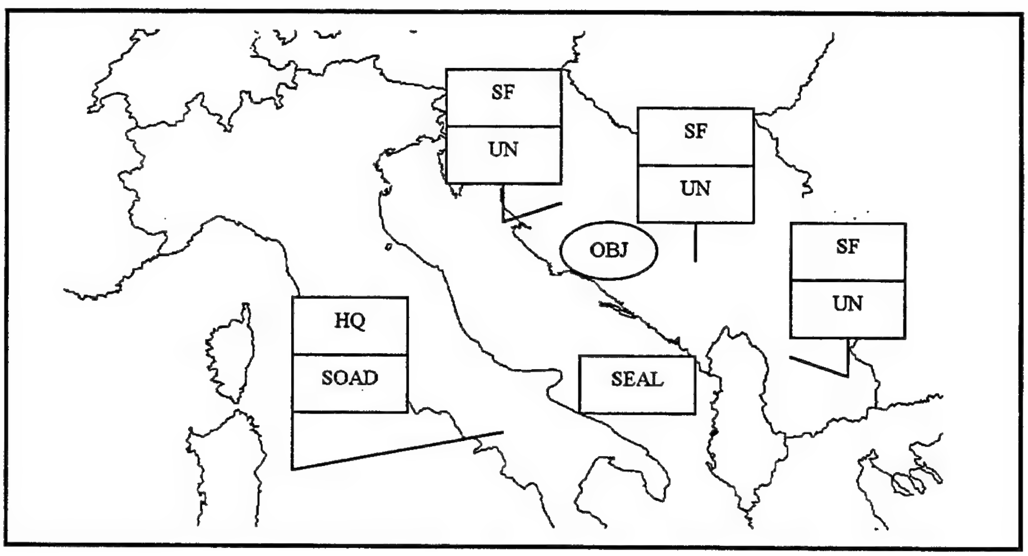

Figure 1. Position of Special Operation Forces

SITUATION: A Serbian Radar site is tracking UN aircraft and needs to be destroyed. The site is in the vicinity of several truck-mounted Serbian forces. The Serbs can be expected to defend the site if they believe it is in danger.

MISSION: The JSOTF will conduct a raid into Bosnia to destroy the radar site.

CONCEPT OF THE OPERATION: The plan is simply as follows – the SOAD located in Italy will pick up the SEALs with 3 x MH-54 helicopters. They will fly the SEALs to the radar site. The SEALs will emplace demolition charges, destroy the radar, and return to the ship via helicopter. The SF and UN forces will move discretely to establish blocking positions on the roads between the objective and Serbian forces, thereby isolating the objective.

PLANNING HARDWARE AND CONNECTIVITY: The operators involved in this mission have a large variety of computer hardware, as shown in Figure 2.

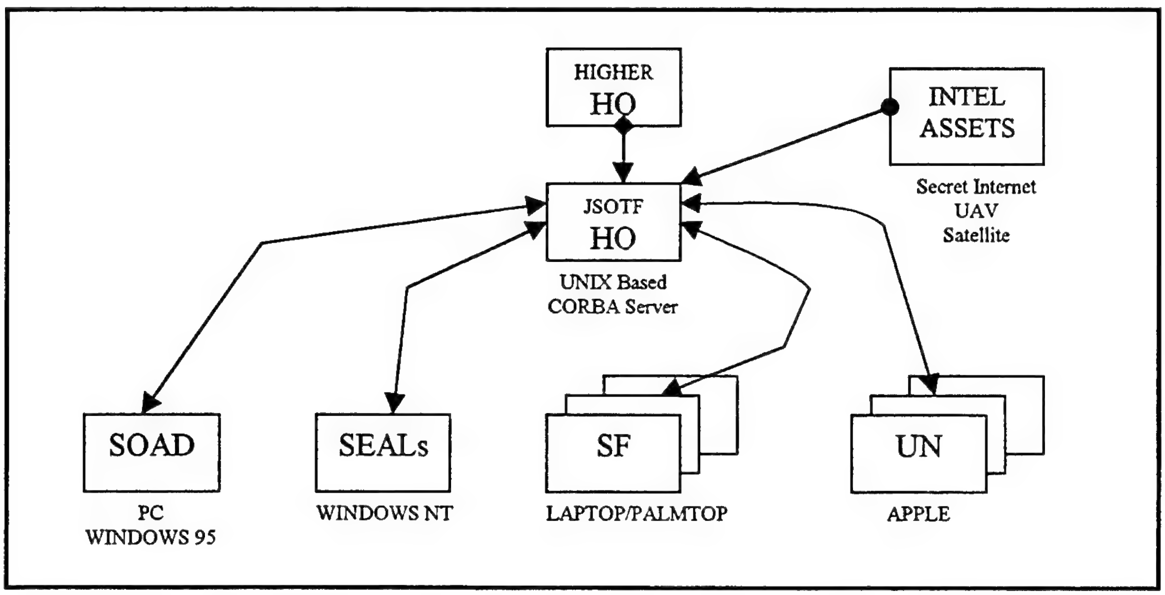

Figure 2. Distributed Planning Computer Platforms

AREA OF OPERATIONS: The following 1:50,000 map shows the area that will be used for this operation.

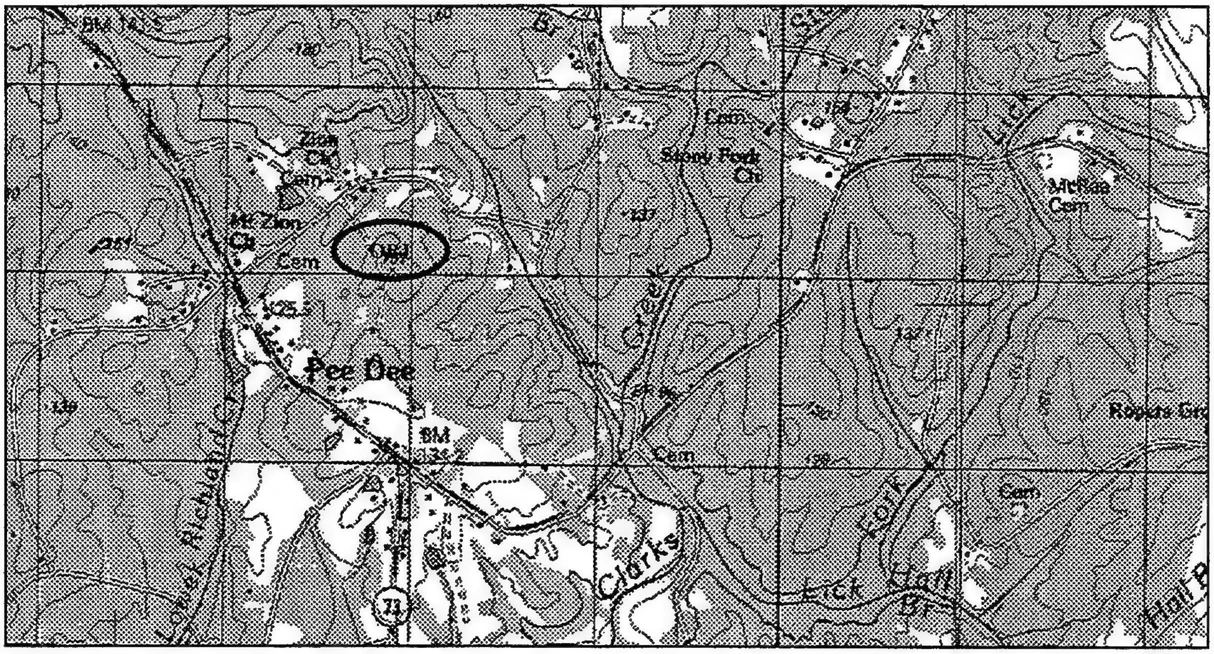

Figure 3. Area of Operations

This scenario shows the very real possibility of planning and conducting a mission with very diverse forces, dispersed over a large area of operations, working on different computing platforms. To plan a mission such as this the planning system must be platform independent, distributed, extensible, and flexible.

APPENDIX B. MAP-BASED PLANNING SYSTEM

This is a simple walk through of the map-based planning system developed to validate the architecture. The name of this system is Special Operation Forces/Loosely Coupled Components (SOFLCC).

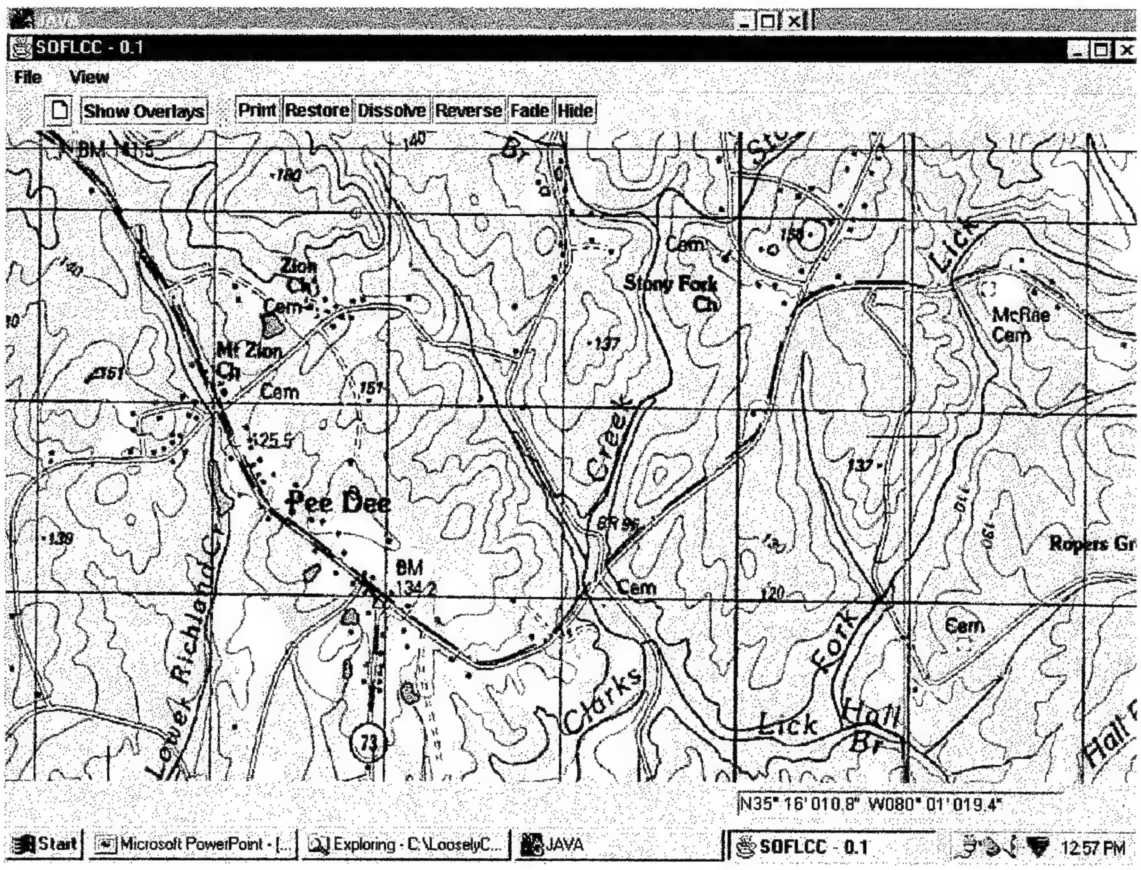

Figure 4. The standard system. This is SOFLCC running in Windows 95. The map is the area of operations which was imported into the system.

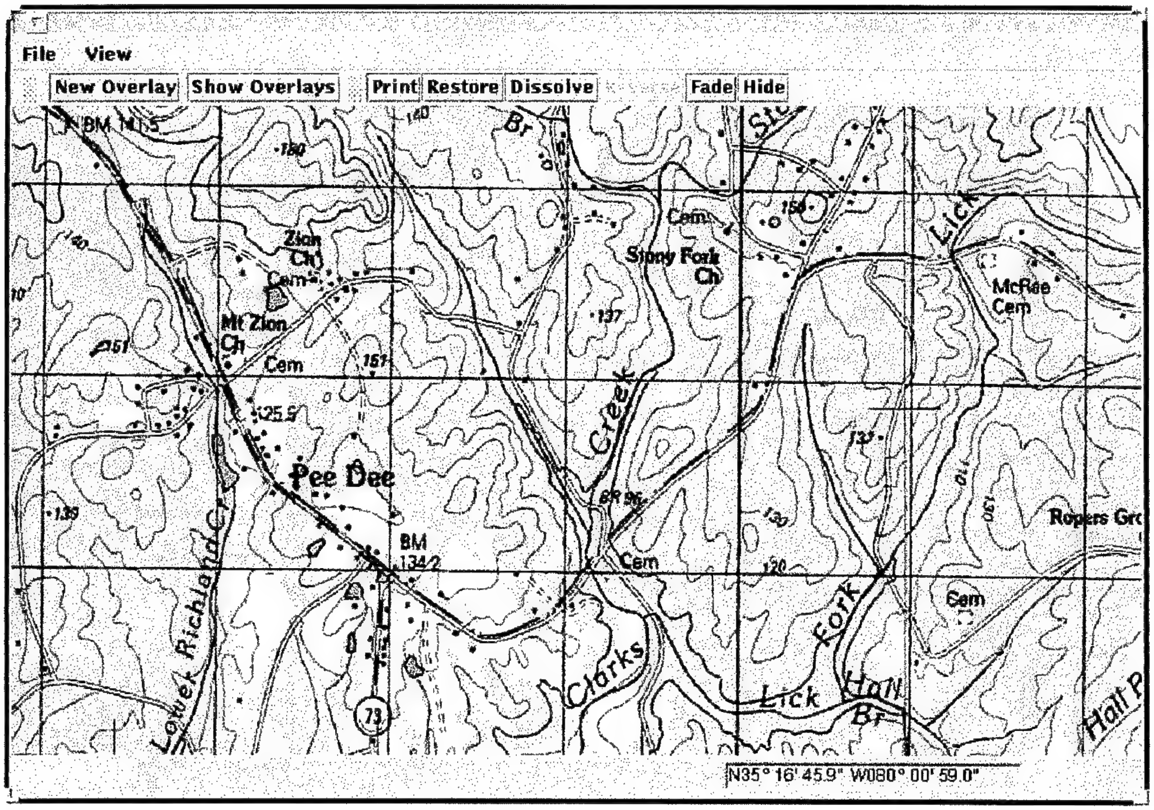

Figure 5. Sun System. This is the same system running on a Sun workstation. The new version of Java gives the same look and feel for each platform.

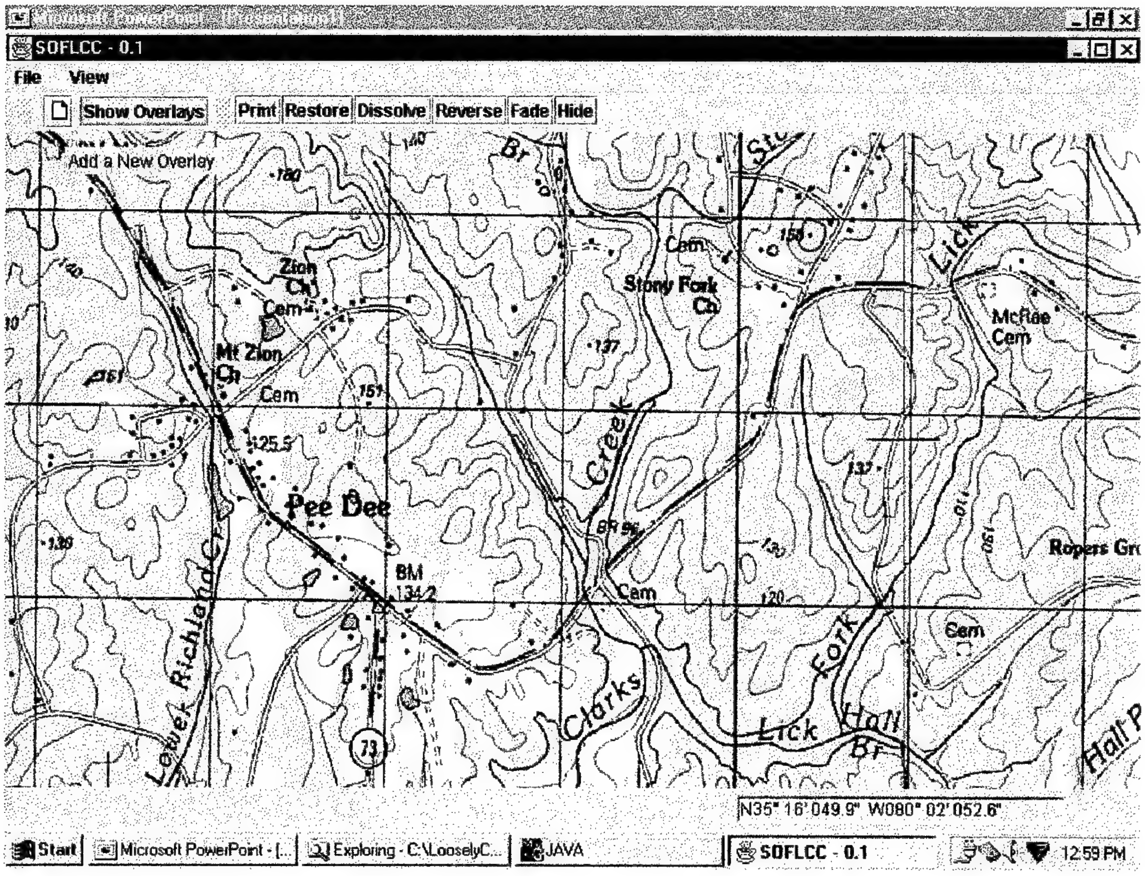

Figure 6. Adding Overlays. To add overlays to the map, click the "Add a New Overlay" icon.

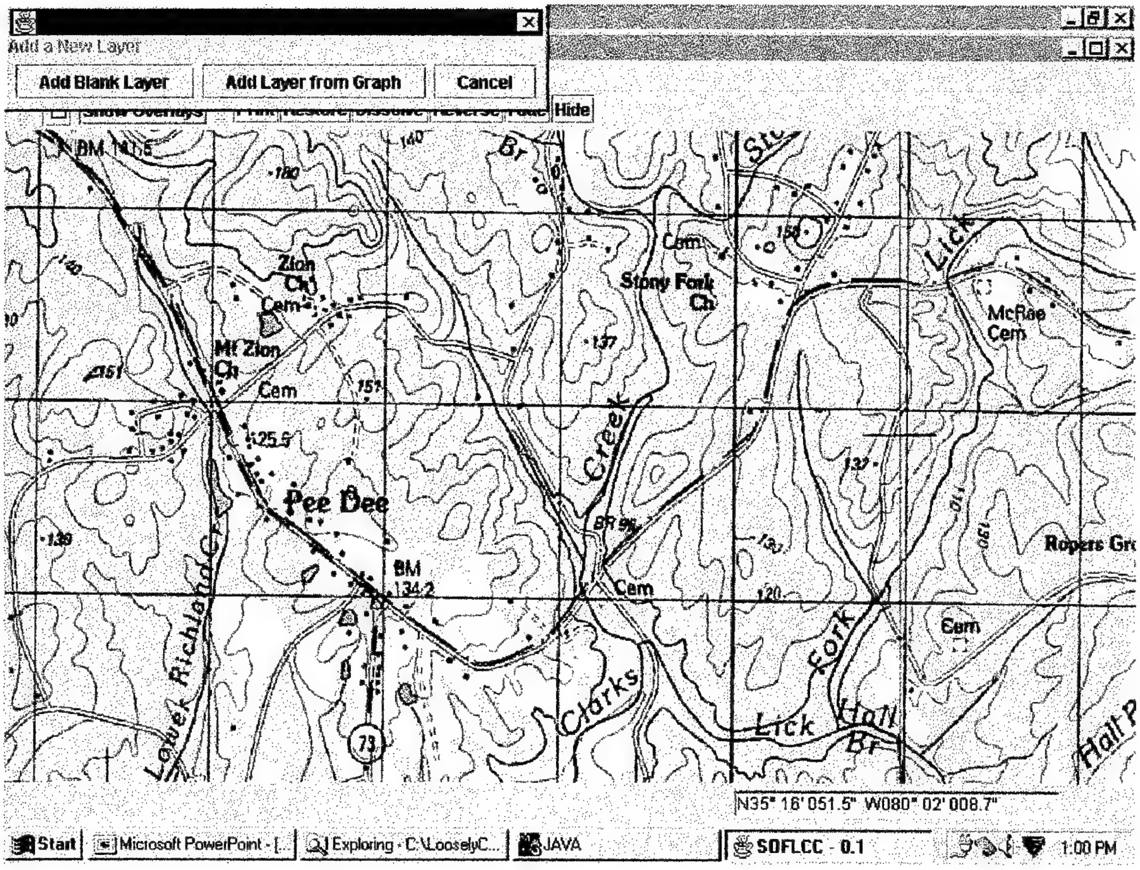

Figure 7. Overlay Dialogue Box. The overlay dialog box gives a choice of overlays.

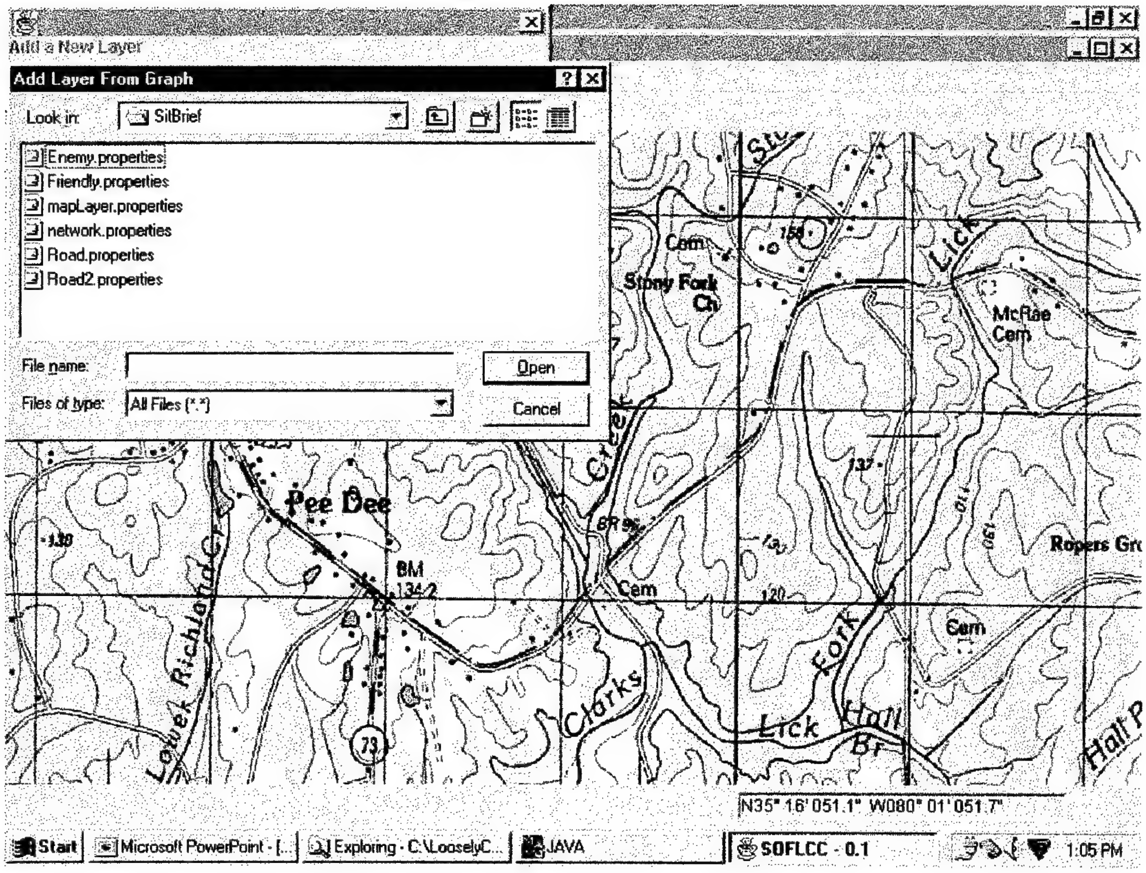

Figure 8. Overlay Files. The system allows the planner to get the overlay from anywhere. In this case it comes from the hard drive, but it could easily come from any network site.

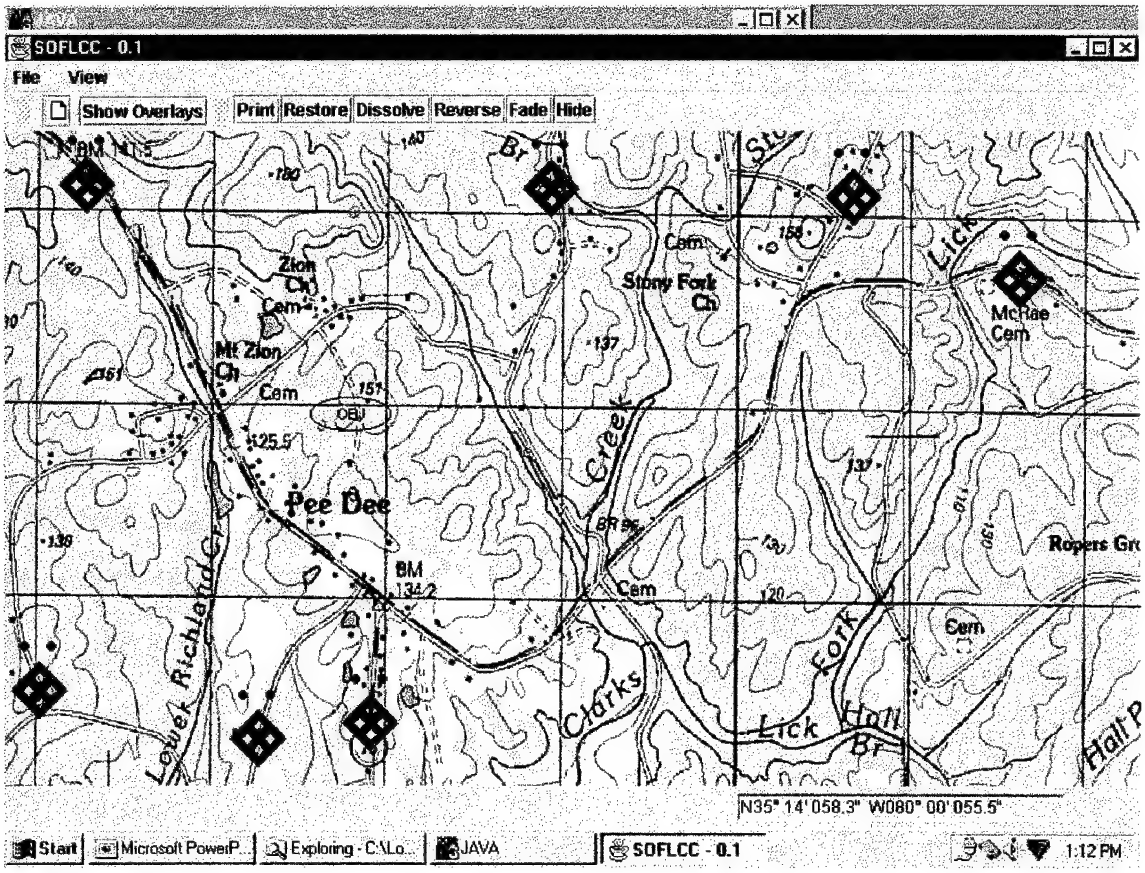

Figure 9. Enemy Situation. SOFLCC now displays the retrieved enemy overlay.

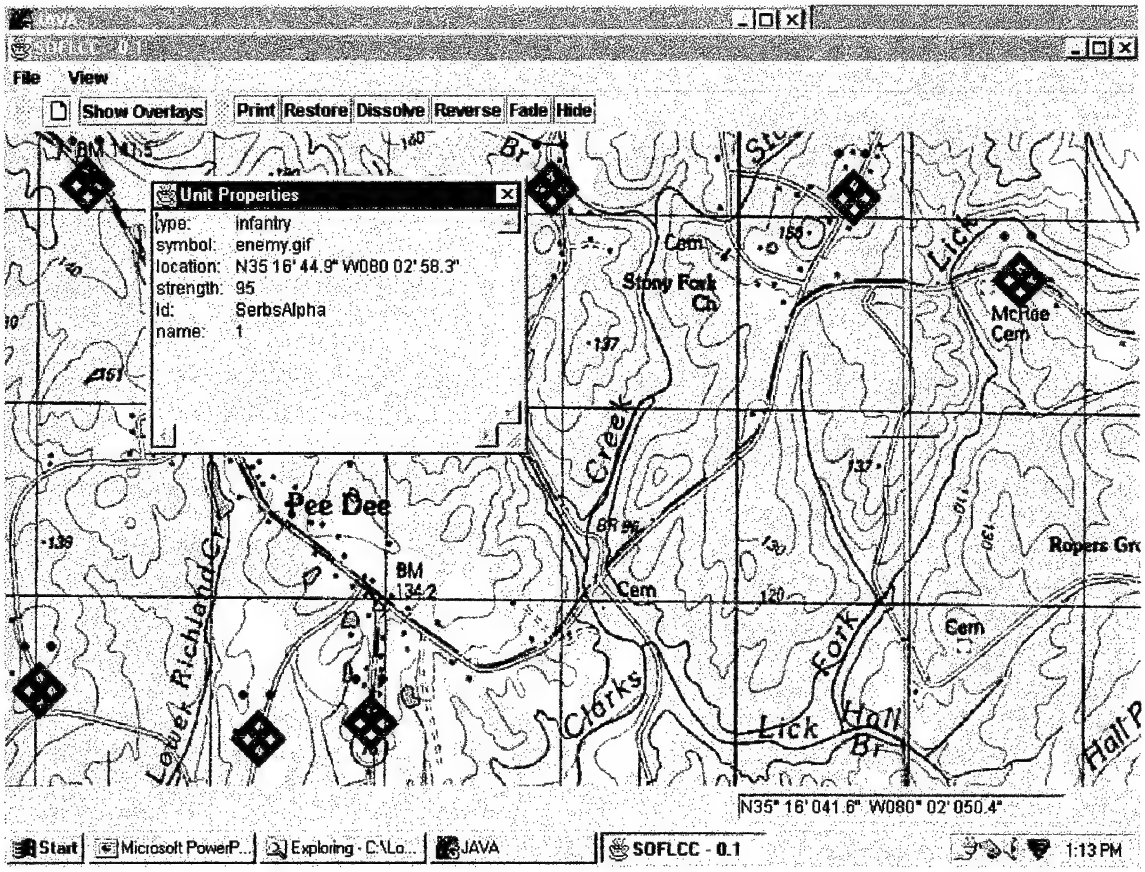

Figure 10. Live Nodes. A key point with SOFLCC is the images are not just mere icons but they are actual nodes. These nodes have properties that are essential to the military planner.

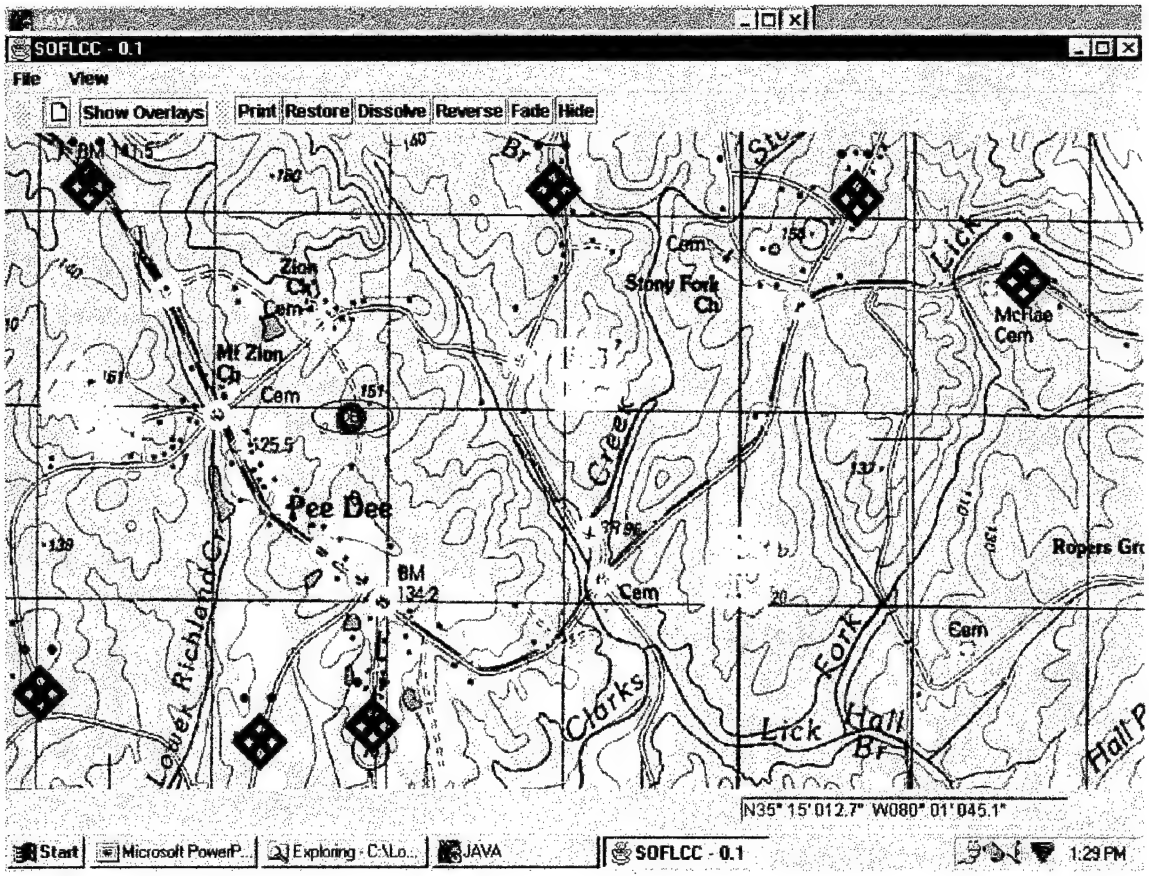

Figure 11. Other Overlays. SOFLCC now displays the friendly situation and road-analysis overlays. The military analyst can add as many overlays as are necessary for the planning process.

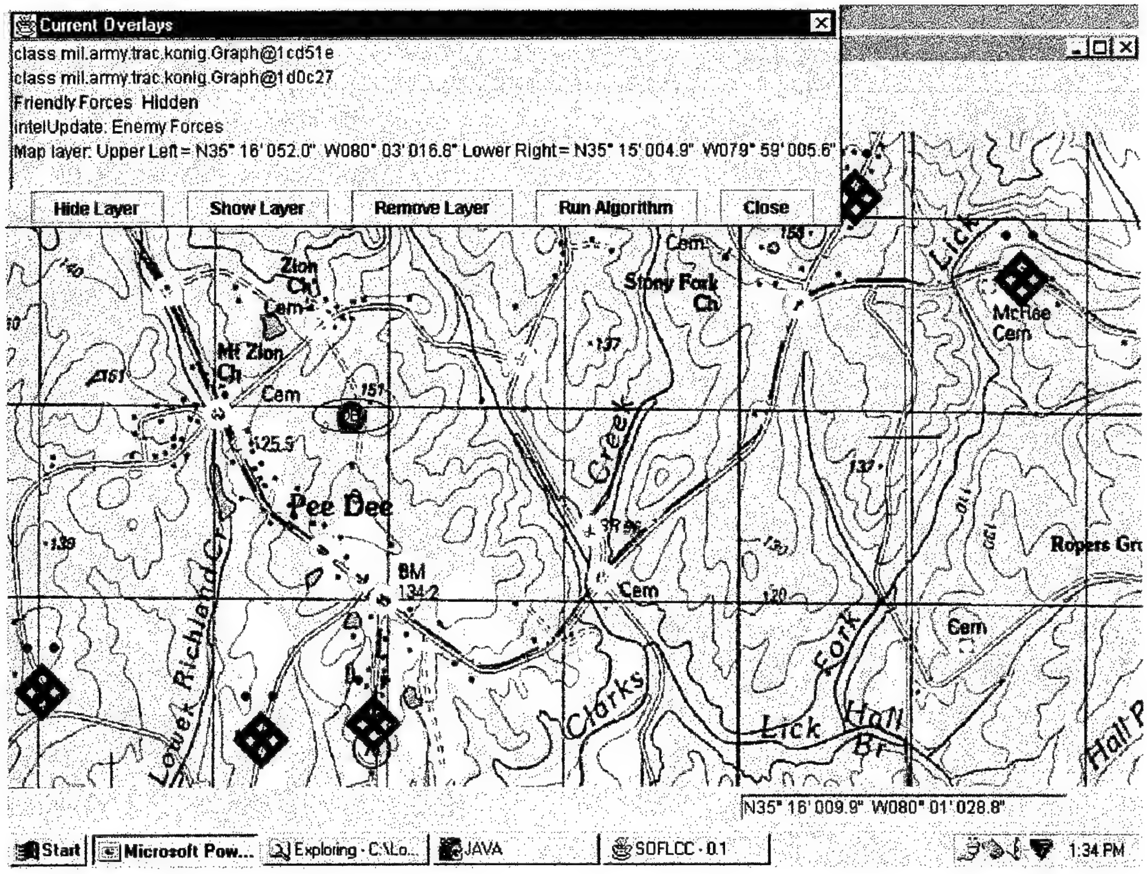

Figure 12. Hide Overlays. These maps have a tendency to become crowded, so SOFLCC has incorporated the ability to remove overlays. In this case the friendly overlay has been hidden.

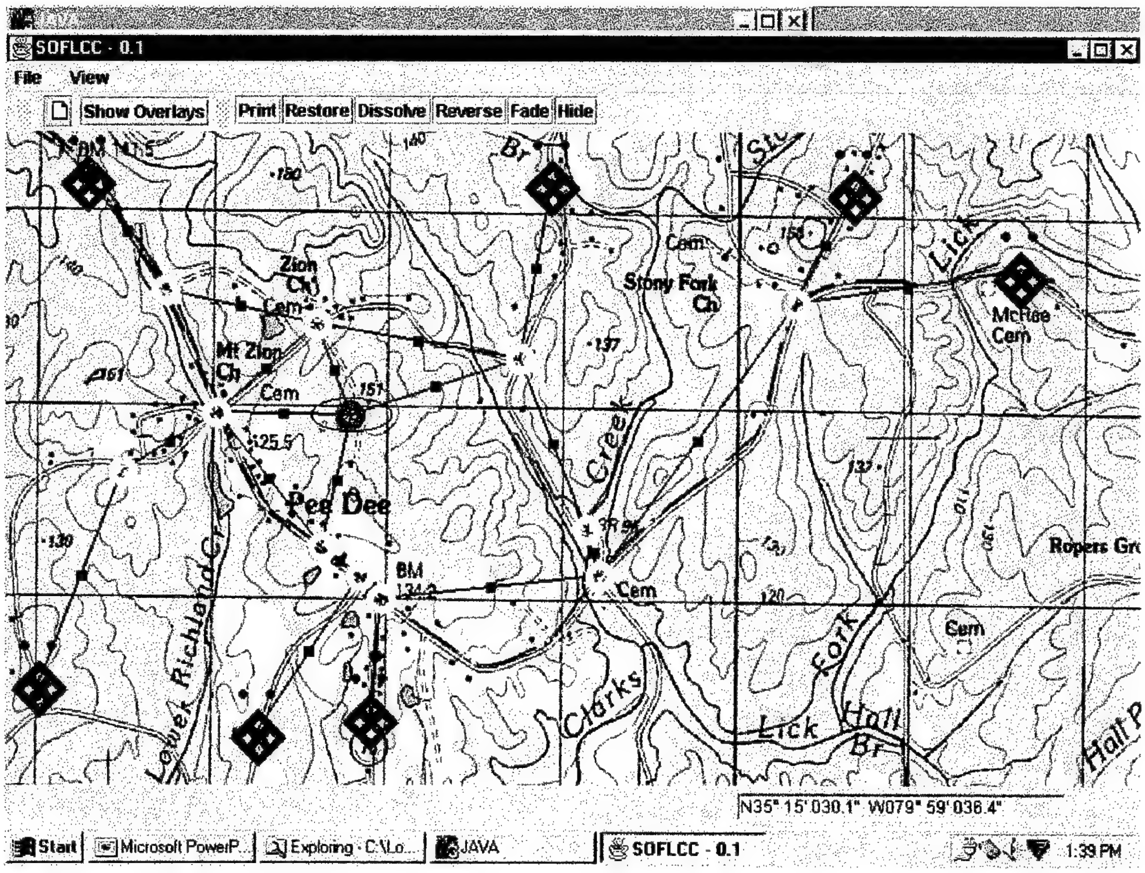

Figure 13. Network. The road intersections can be connected to the enemy nodes to create a graph network. In this scenario, a military analyst has constructed this network from the various overlays. The military intelligence analyst wants to determine the shortest path from each enemy node to the objective. The commander of this operation wants to afford the most time on the objective for the SEALs. He will want to use the SF and UN forces to establish road blocks. Obviously, the commander will want to block the enemy that can get to the objective in the shortest amount of time.

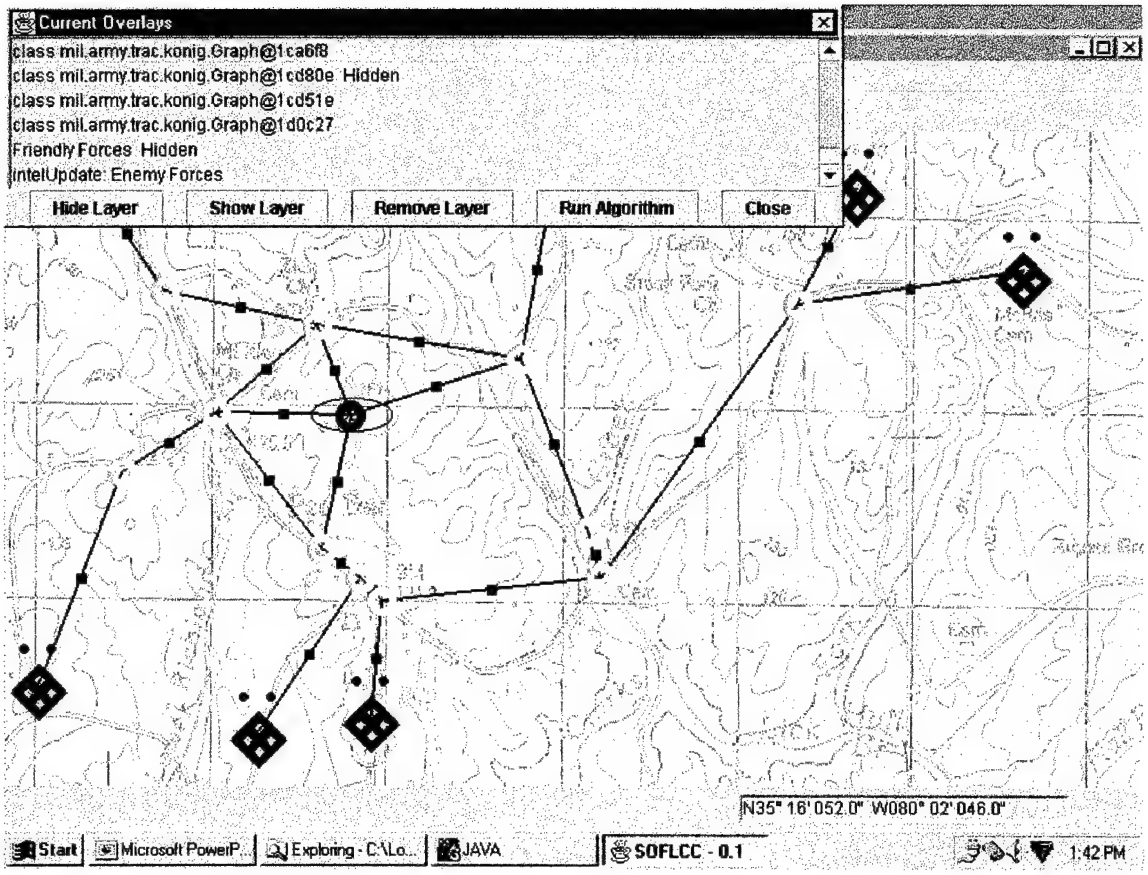

Figure 14. The military analyst has found a network algorithm component and has added it to the SOFLCC planning and analysis system. The architecture has allowed him to do this. The algorithm component will have its own graphic user interfaces (GUI) and will guide the analyst through the input of data.

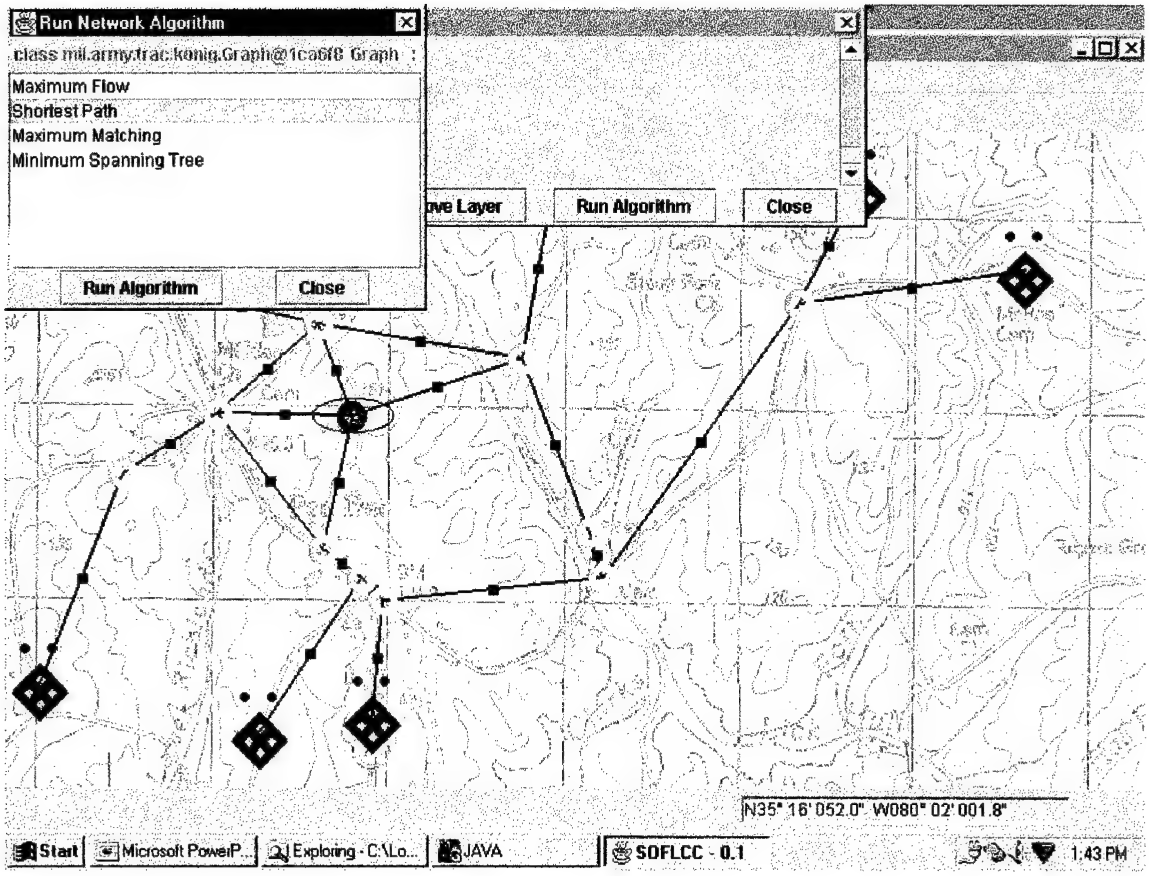

Figure 15. Network Algorithm Component. In this particular case, the algorithm component offers the possibility of running different types of algorithms.

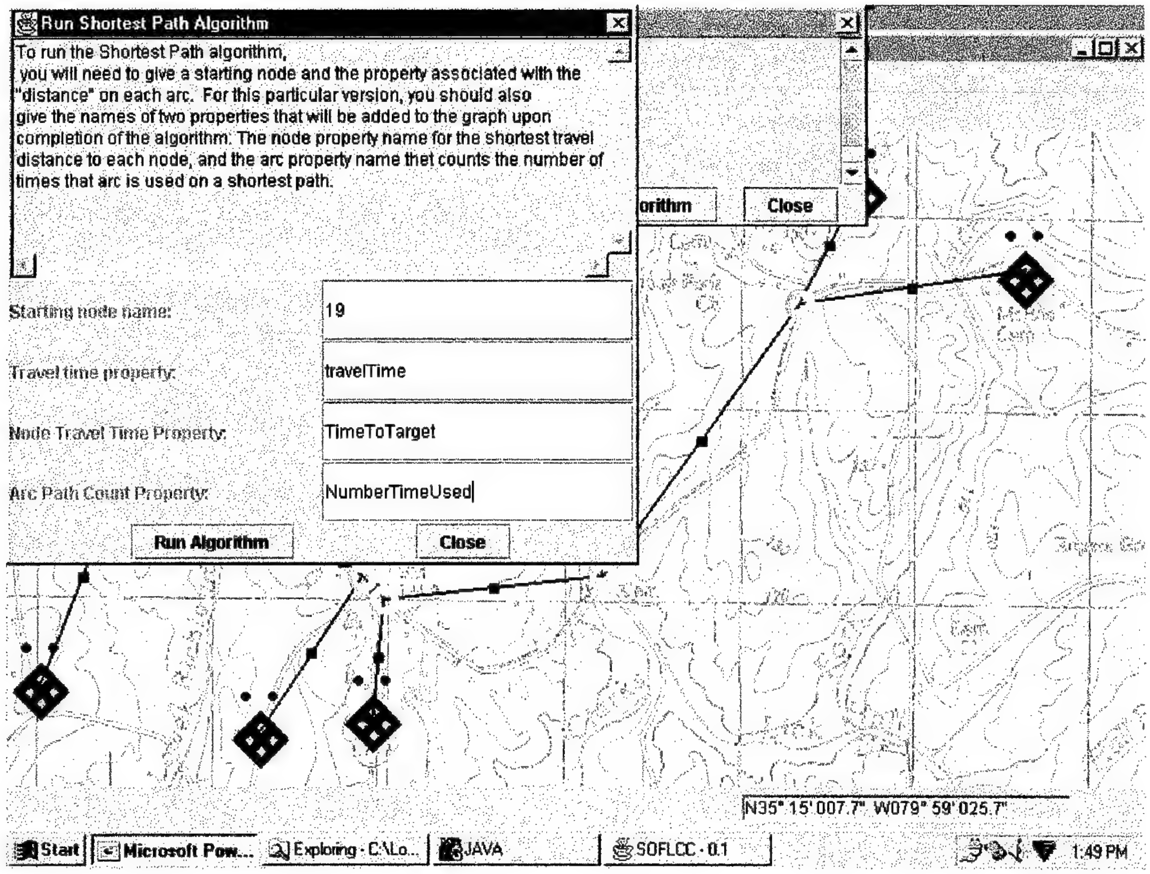

Figure 16. Algorithm Description. This algorithm component includes a brief description and instructions.

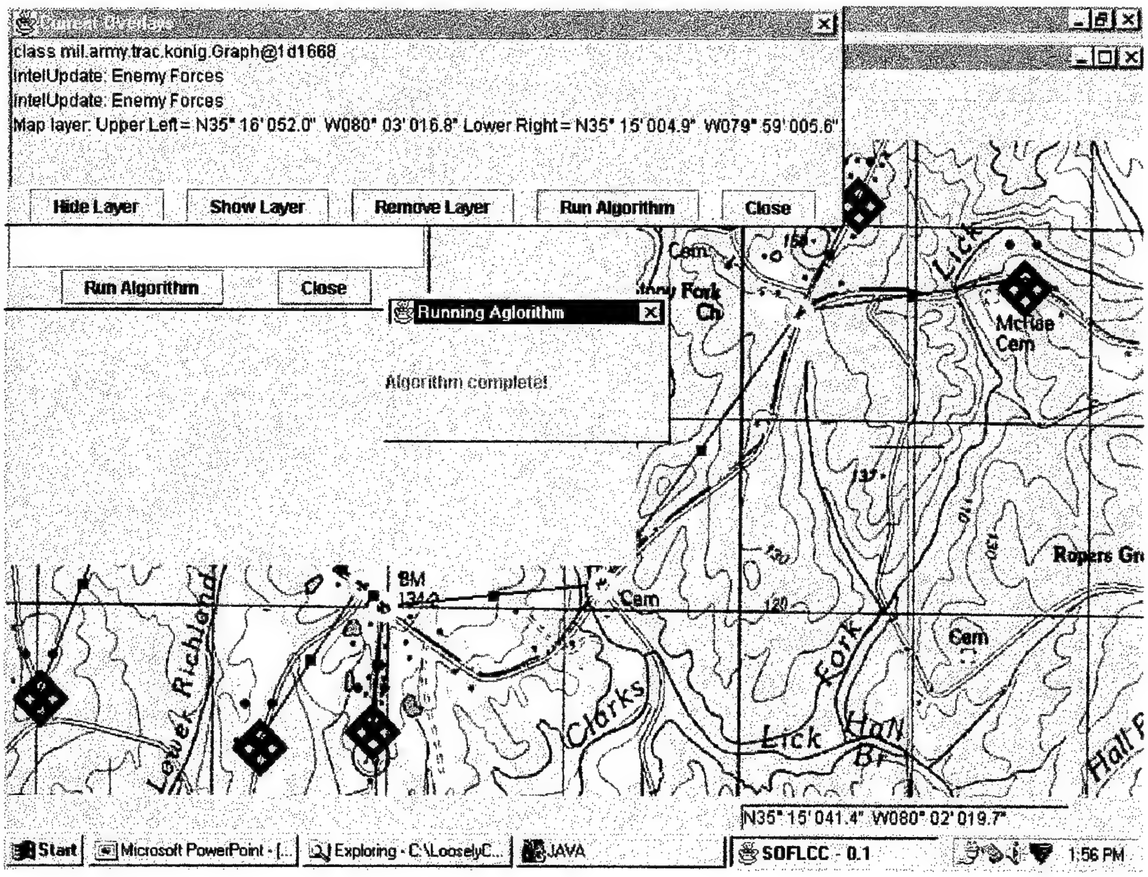

Figure 17. Algorithm Complete. The algorithm is complete and the results are now posted in the properties list for each node.

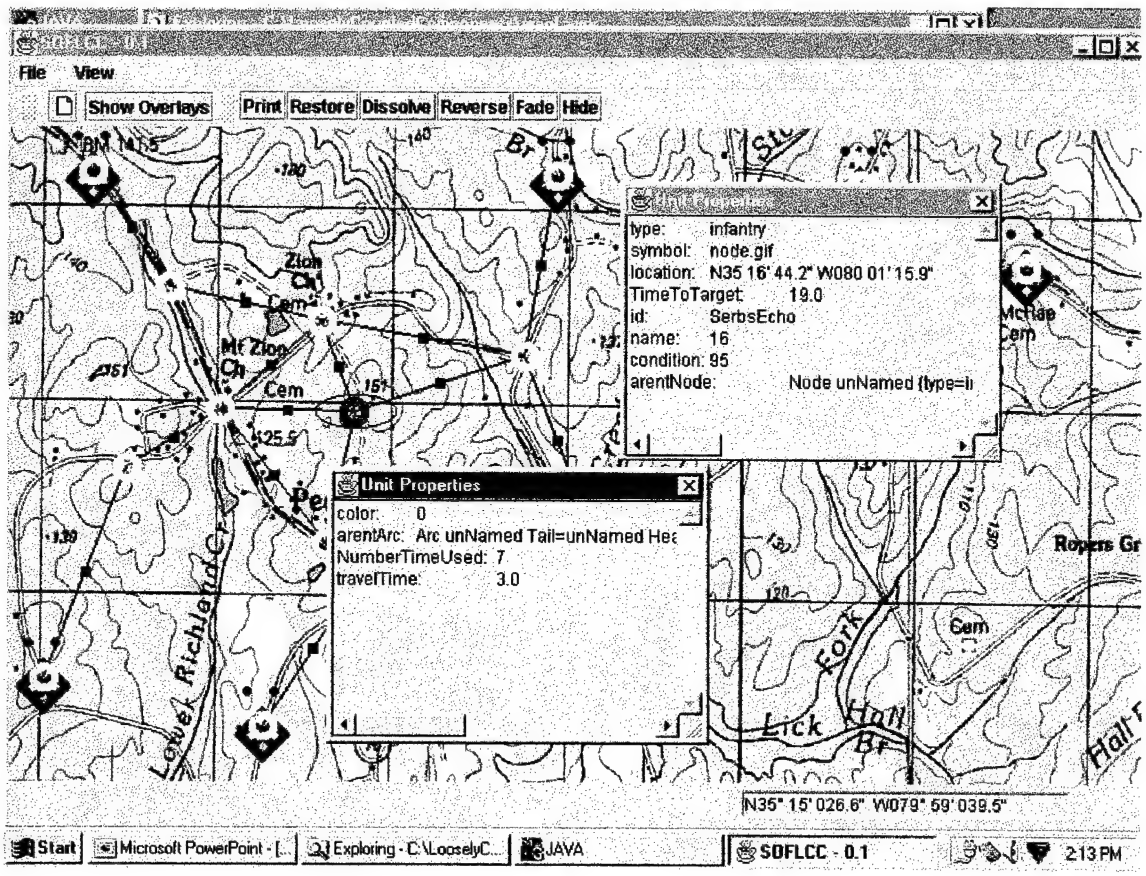

Figure 18. Information Display. The algorithm has determined the minimum travel time for each enemy node to the objective. This information has now been added to the properties list for each enemy node. Additionally, each arc or road properties list has the number of times each arc has been used. This information would tell the military analyst which roads were used the most and which enemy could get to the objective in the shortest amount of time.

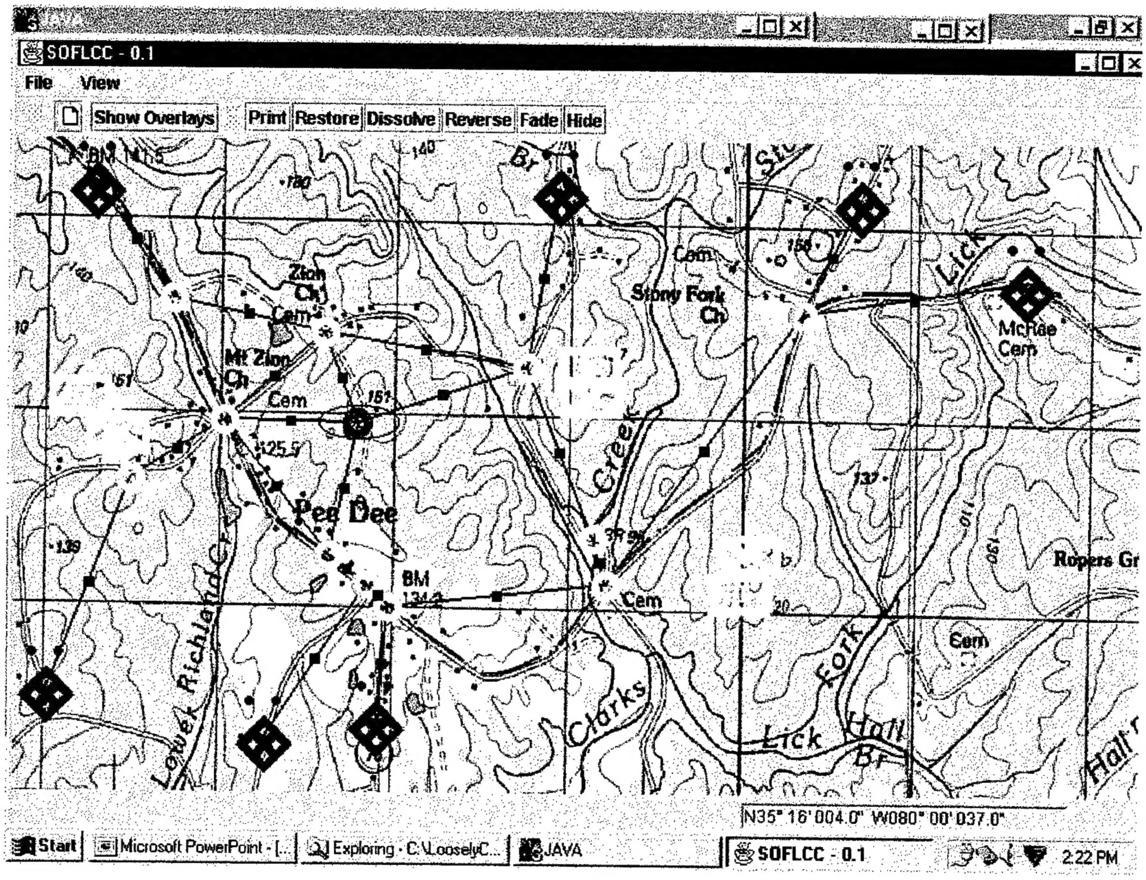

Figure 19. Other Algorithms. The information already displayed can help the commander of this operation determine where to emplace the friendly forces in road block positions. Additional OR algorithms could be added to the SOFLCC system to assist the military analyst.

LIST OF REFERENCES

[1] Chairman of the Joint Chiefs of Staff. (1996). Joint Vision 2010: America's Military: Preparing for Tomorrow, 5126 Joint Staff, Pentagon, Washington D. C.

[2] Commander in Chief, United States Special Operations Command. (1996). SOF Vision 2020, MacDill, Air Force Base, Tampa, FL.

[3] Bradley, G.H. and Buss, A.H. (1998). An Architecture for Dynamic Planning Systems Using Loosely coupled Components. Technical Report, Naval Postgraduate School, Monterey, CA.

[4] Defense Information Systems Agency. (1998) "Mission and Mandate," http://www.disa.mil/missman.html.

[5] Chairman of the Joint Chiefs of Staff. (1996) Global Command and Control System, Joint Staff, Pentagon, Washington D. C.

[6] Joint Interoperability Test Command. (1996). General Information and Defense Information Infrastructure (DII) Distributed Test Network. [Brochure] Fort Huachuca, AZ.

[7] Secretary of the Army. (1997). Force XXI: America's Army in Transition, U.S. Army Training and Doctrine Command, Fort Monroe, VA.

[8] Spooner, Socorro. (1998). "Soldiers and commanders benefit from new technology," 14th Public Affairs Detachment, http://www-tradoc.army.mil/pao/newtech.htm, May 1998.

[9] Chief of Staff, U.S. Air Force, "Global Engagement: A vision of the 21st Century Air Force," http://www.af-future.hq.af.mil/21/nuvis.htm, January 1997.

[10] DTAI, Incorporated, "Enhanced Common Operational Picture," http://mycroft.nosc.mil/v2/ECOP, February 1998.

[11] Seaton, S. and Arnold, J. (1998). InCON A New Generation of Tactical Command and Control from SRI International. SRI International, Menlo Park, CA.

[12] McSwain, D.W., CDR. (1997). COMPASS Project. Naval Research and Development Center, San Diego, CA.

[13] NCCOSC RDT&E Division. (1997). Common Operational Modeling, Planning and Simulation Strategy, Post Exercise Report for SOCOM Support for Roving Sands 97 Command Post Exercise, 14-25 April 1997. San Diego, CA.

[14] Air Force Information Warfare Center. (1997) Information Operations Planning Tool Development Status (Program Status Report). Kirkland AFB, NM.

[15] Defense Advanced Research Projects Agency. (1998). Special Operations Forces Planning (SOFPLAN (TIE97-3)). APRI Demonstrations May 6-8, 1998 [Brochure]. Monterey, CA. Major D. E. Dyer.

[16] Morse, P. and Kimball, G. (1951). Methods of Operations Research , John Wiley and Sons, New York. Taken from article by Washburn, A. (1996). The Teachers' Forum: The Operations Analysis Curriculum at the Naval Postgraduate School. Interfaces, 26, 71-80.

[17] Halfhill, T. R. (1998). How to Soup up Java, Part I. BYTE, 60-74.

[18] Cornell, G. and Horstmann, C.S. (1996). Core Java. Mountain View, CA: SunSoft Press.

[19] Orfali, R., Harkey, D., and Edwards, J. (1997). Instant CORBA. John Wiley and Sons, New York.

[20] Edwards, Sean J. A. (1997). The Threat of High Altitude Electromagnetic Pulse to Force XXI. National Security Studies Quarterly, II, 61-80.

[21] Arquilla, J. (1998) "High Powered Microwaves," Information Operations Course for the Special Operations, Low Intensity Conflict curriculum at the Naval Postgraduate School, April 27.

[22] Hundley, R. O. and Anderson, R.H. (1996). Emerging Challenge Security and Safety in Cyberspace. RAND Reprints, Santa Monica, CA (Reprinted from IEEE Technology and Society Magazine, Vol. 14, No.4, Winter 1995-1996, pp.19-28.

[23] Introduction to Computer Security (1997). Monterey, CA: Naval Postgraduate School.

[24] Brown, Andrew. S-Tools [Computer software]. (1996). West Yorkshire, UK

[25] Sun Microsystems, Inc., "Sun Premieres Java Cryptography Toolkit," http://www.javasoft.com/pr/1998/01/pr980112.html, April 1998.

INITIAL DISTRIBUTION LIST

No. Copies

1. Defense Technical Information Center..2
   8725 John J. Kingman Rd., STE 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library..2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Professor Gordon Bradley, Code OR/BZ......................................4
   Department of Operations Research
   Naval Postgraduate School
   Monterey, CA 93940-5000

4. LTC Charles Shaw, III, Code OR/SC..1
   Department of Operation Research
   Naval Postgraduate School
   Monterey, CA 93940-5000

5. U.S. Special Operations Command..3
   ATTN: J7
   7701 Tampa Point Blvd
   MacDill AFB, FL 33621-5323

6. CPT (P) Al Bilyeu..1
   24 East Taylor Street
   Savannah, GA 31401

7. Headquarters, Department of the Army.......................................1
   Deputy Undersecretary of the Army (Operations Research)
   ATTN: Walter W. Hollis
   102 Army Pentagon
   Washington D.C. 20310-0102